

Fortinet.Certkiller.FCESP.v2014-11-11.by.Oaken.81q

Number: FCESP
Passing Score: 500
Time Limit: 162 min
File Version: 28.5

Exam Code: FCESP

Exam Name: Fortinet Certified Email Security Professional



CERTKILLER
slay your exams

FCESP

QUESTION 1

Which protection profile can be used to protect against Directory Harvest attacks?

- A. antispam profile
- B. session profile
- C. content profile
- D. antivirus profile

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

What is one reason for deploying a FortiMail unit in Transparent Mode?

- A. DNS records do not necessarily have to be modified.
- B. Mail is not queued thereby expediting mail delivery.
- C. Mail is not inspected unless a policy explicitly matches the traffic.
- D. No user information needs to be stored on the FortiMail unit when operating in Transparent Mode.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Which profile can be used to protect against Denial of Service attacks?

- A. antispam profile
- B. session profile
- C. dos profile
- D. security profile

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Which of the following parameters CANNOT be configured using the Quick Start Wizard?

- A. protected domains
- B. system time
- C. operation mode
- D. access control rules
- E. antispam settings

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Which of the following DNS records resolves an IP address into a hostname?

- A. MX record
- B. PTR record
- C. A record
- D. NS record

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Which SMTP sessions are defined as incoming?

- A. All SMTP sessions received by the FortiMail units
- B. SMTP sessions for the protected domain
- C. SMTP sessions received on the management interface
- D. All sessions generated from the internal network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Which back-end servers can be used to provide Recipient Verification?

- A. LDAP servers
- B. POP3 servers
- C. RADIUS servers
- D. SMTP servers

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Under which of the following conditions would an email be placed in the Dead Mail queue?

- A. The recipient of the email is invalid.
- B. The sender of the email is invalid.
- C. The email is classified as spam.
- D. The remote MTA is performing Greylisting.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

A System Administrator is concerned by the amount of disk space being used to store quarantine email messages for non-existent accounts. Which of the following techniques can be used on a FortiMail unit to PREVENT email messages from being quarantined for non-existent accounts?

- A. Greylist Scanning
- B. Recipient Address Verification
- C. Sender Reputation
- D. Automatic Removal of Invalid Quarantine Accounts

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Which of the following features can be used to expand a single recipient address into a group of one or many email addresses?

- A. User Alias
- B. Address Map
- C. User Group
- D. None of the above

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

On a FortiMail unit, access control rules specify actions to be taken against matching email messages. Which of the following statements correctly describes the Bypass action?

- A. Accept the email message but skip the MX record lookup. This mail message will be delivered using the configured relay server.
- B. Do not deliver the email message.
- C. Accept the email message and skip all message scanning, such as antispam and antivirus.

D. Accept the email message and delete it immediately without delivery.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which of the following FortiMail profile types apply to IP-based policies only?

- A. Session profile
- B. Content profile
- C. IP pool
- D. Antispam profile

Correct Answer: AC

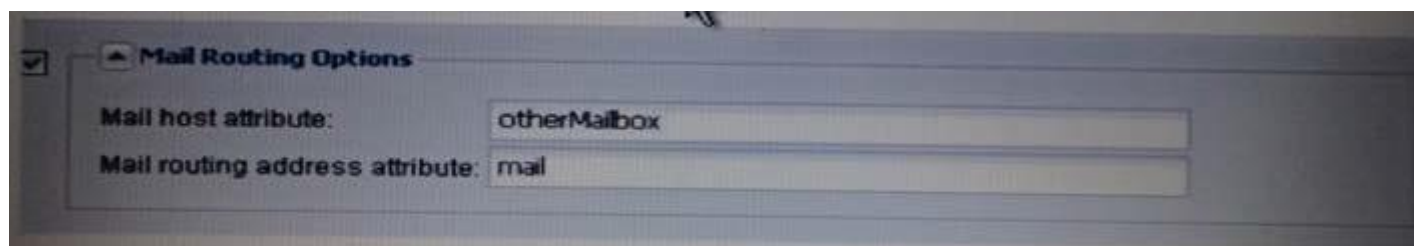
Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

In the exhibit, what is the role of the Mail host attribute?



- A. It indicates the MTA to which email should be sent.
- B. It contains the recipient email address used to trigger the mail routing.
- C. It indicates to which alias email address the email should be redirected.
- D. It indicates which MTA should have sent this mail message. Mail sent from another MTA is considered spam.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

In the local storage structure of the FortiMail unit, what does the flash memory contain?

- A. Firmware Image
- B. System Configuration
- C. History Log
- D. Event Log
- E. User Data
- F. Certificates

Correct Answer: ABF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

When the DomainKeys Identified Mail (DKIM) feature is used, where is the public key stored?

- A. The public key is stored on the central CA.
- B. The public key is distributed automatically during the SMTP session establishment.
- C. The public key is stored in the DNS TXT record.
- D. The public key is stored in the DNS PTR record.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which of the following statements regarding Antivirus scanning is NOT correct?

- A. Antivirus scanning is performed on incoming email traffic only.
- B. When a virus is found, the infected file is replaced with a replacement message.
- C. An SMTP session that matches an Access Control Rule with action Bypass is exempted by Antivirus scan.
- D. When an email is detected as infected, the Sender Reputation score associated with the sender IP is incremented.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

A FortiMail unit is installed in Gateway mode and is protecting a single email domain. Which of the following statements is NOT true in this scenario?

- A. An incoming recipient-based policy can be used to apply scanning to email messages destined to the protected domain.
- B. The DNS MX record for the protected domain must point to the FortiMail unit FQDN for incoming SMTP email messages to be scanned.
- C. The mail server or email clients must use the FortiMail unit as the SMTP relay to enable scanning of outgoing SMTP email messages.
- D. An access control list entry must be configured to allow the FortiMail unit to relay incoming traffic to the protected domain.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

According to the Message Header printed below, which antispam technique detected this email as spam:

Return-Path: user1@external.lab
(SquirrelMail authenticated user user1)
by 172.16.78.8 with HTTP;
X-FEAS-HASH: 6ef419f0a0608b1655xxxxe68080df3cb12fc38f1118d2f085985eeb000274d7
Sat, 18 Apr 2009 15:53:06 +0200 (CEST)
Message-ID : <3029.192.168.3.101.1240062786.squirrel@172.16.78.8>
Date : Sat, 18 Apr 2009 15 :53 :06 +0200 (CEST)
Subject: [SPAM] Sales
From: user1@external.lab

To: user1@training1.lab
User-Agent: SquirrelMail/1.4.10a-1.fc6
MIME-Version : 1.0
Content-Type : text/plain ;charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal
X-Original-To: user1@training1.lab
Delivered-To: user1@training1.lab
Received: from fm.sub.training1.lab (fm.sub.training1.lab [192.168.11.101])
by mail.training1.lab (Postfix) with ESMTP id A9160187073
for <user1@training1.lab>; Sun, 19 Apr 2009 16:58:48 +0200 (CEST)
Received: from mail.external.lab ([172.16.78.8])
by fm.sub.training1.lab with ESMTP id n3LEPHWu001093
for <user1@training1.lab>; Tue, 21 Apr 2009 10:25:17 -0400
Received: from 172.16.78.8 (localhost [127.0.0.1])
by mail.external.lab (Postfix) with ESMTP id 247D9BF893
for <user1@training1.lab>; Sat, 18 Apr 2009 15:53:06 +0200 (CEST)
Received: from 192.168.3.101

- A. DNSBL scan
- B. Dictionary scan
- C. Banned Word scan
- D. FortiGuard checksum

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

A FortiMail administrator has added a Virtual IP address to the port2 interface of an Active Passive Cluster. Which of the following statements is true regarding this scenario?

- A. The master unit can be reached using both physical IP and virtual IP addresses.
- B. The master unit can be reached only by using its physical IP address.
- C. The virtual IP address is always associated to the active master of a cluster.
- D. The virtual IP address overrides the physical IP address.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

What is the SMTP command used to initiate SMTP authentication?

- A. AUTH LOGIN
- B. START TLS
- C. LOGIN
- D. DSN

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A System Administrator is concerned by the amount of system resources being used to store quarantine email messages for non-existent accounts. Which of the following techniques can be used on a FortiMail unit to free up system resources?

- A. Greylist scanning
- B. Recipient Address Verification
- C. Sender Reputation
- D. Automatic Removal of Invalid Quarantine Accounts

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

How can a FortiMail administrator view or search archived emails?

- A. through POP3, IMAP or Web-based manager
- B. through POP3 and IMAP
- C. through Webmail only
- D. through Web-based manager only

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

What is the recommended procedure to identify emails encoded in a specific charset?

- A. Configure a Dictionary profile entry and associate it to the content profile section Content Monitor and Filtering.
- B. Create a banned word entry in an Antispam profile.
- C. Charset encoding cannot be detected.
- D. Enable Heuristic Scanning in an Antivirus profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Which of the following back-end servers can NOT be used to provide Recipient Verification?

- A. LDAP servers
- B. POP3 servers
- C. RADIUS servers
- D. SMTP servers

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Which of the following statements is true regarding Session-based antispam techniques?

- A. The entire mail content is inspected.
- B. They are enabled in the session profile only.
- C. SMTP commands, sender domain and IP address are checked.
- D. They are checked after application-based antispam techniques.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

A FortiMail administrator must enforce the following company policy:

1. All emails containing executable attachments must be detected.
2. This detection must be file name independent. For example, if a user renames an executable from .exe to .txt, the file should still be detected.

Which FortiMail inspection technique should the administrator apply?

- A. Content profile > Attachment filtering rule to block all executable extensions
- B. Content profile > File Type filtering rule to block all executable files
- C. Antispam profile > Banned Word entry to block all executable files
- D. Content profile > Content Monitor entry to block all executable files

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Two access control rules are configured on a FortiMail unit as illustrated in the exhibit.

Exhibit

Enabled	ID	Sender Pattern	Recipient Pattern	Sender IP/Netmask	Reverse DNS Pattern	Authentication Status	TLS Profile	Action
<input checked="" type="checkbox"/>	1	-*	-*@internal1.lab	172.16.78.8/255.255.255.255	-*	Any		RELAY
<input checked="" type="checkbox"/>	2	-*@external1.lab	-*	0.0.0.0/0.0.0.0	-*	Any		REJECT

Close

Which of the following statements correctly describes the COMBINED action of these two access control rules?

- A. Email messages from senders at external1.lab will be rejected.
- B. Email messages from external1.lab to internal1.lab from host IP 172.16.78.8 are relayed.
- C. Email messages from external1.lab to internal1.lab from any host IP address are relayed.
- D. Email messages from external1.lab to internal1.lab are restricted by the return DNS pattern.

Correct Answer: B

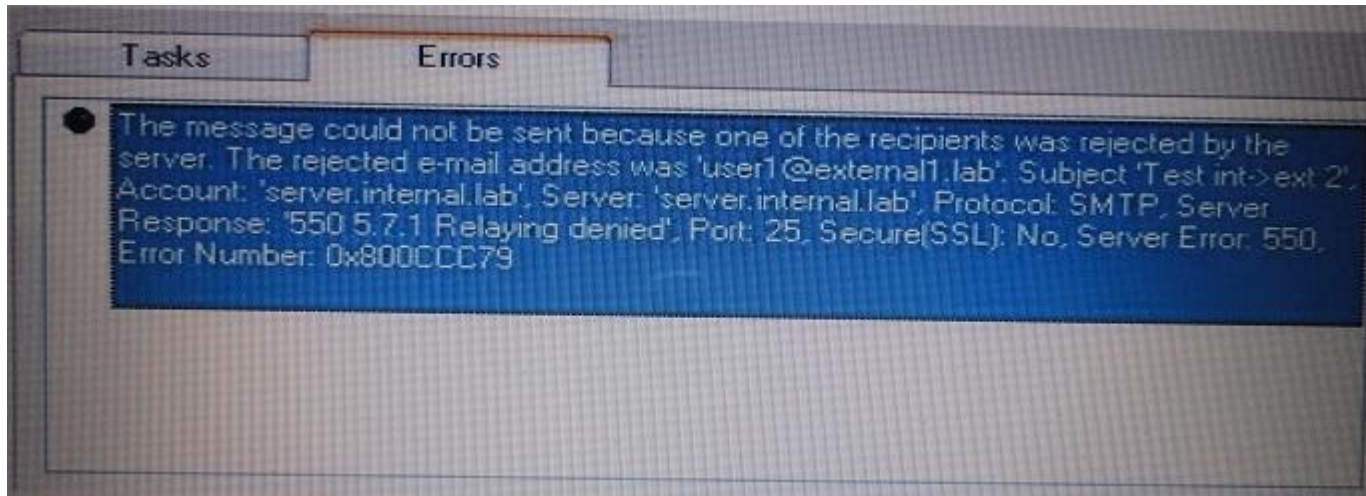
Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

What is the best explanation for why a FortiMail unit would issue the error message indicated in the exhibit?



- A. The recipient domain external1.lab is not defined.
- B. This traffic comes from an authenticated sender.
- C. Recipient verification is not working properly.
- D. The session is matching an Access Control Rule with action "Reject".

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

Which of the following statements regarding the FortiMail unit's Greylisting feature is NOT correct?

- A. The FortiMail unit tracks the /32 bit host address of the sender.
- B. When an email is received from a new sender IP address, envelope sender and envelope recipient addresses, the FortiMail unit will initially send a temporary failure message.
- C. After the initial temporary fail message is sent, the message must be retransmitted between the Greylisting period expiry and initial expiry time periods.
- D. Pass-through is allowed until the configured TTL expires.
- E. An ACL with action Relay bypasses Greylisting.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

Which of the following statements regarding User Quarantine Access is true?

- A. User Quarantine access can be enabled in Recipient-based policies only.
- B. User Quarantine access can be enabled in IP-based policies only.
- C. An authentication profile is only needed when the FortiMail is protecting multiple domains.
- D. Email users can access their quarantine emails through an IMAP client.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Which of the following statements is true regarding Recipient and IP-based policies?

- A. Recipient-based policies are applied to mail sent to specific users. IP-based policies are applied to connections by client IP address in Gateway and Server modes and both client and server IP addresses in Transparent mode.
- B. Recipient-based policies apply to incoming traffic only. IP-based policies apply to both incoming and outgoing traffic.
- C. Recipient-based policies apply to both incoming and outgoing traffic. IP-based policies apply to incoming traffic only.
- D. IP-based Policies always override Recipient-based policies.
- E. Traffic is matched against IP-based policies before being matched against Recipient-based policies.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

An email user reports that his mail client is unable to display correctly all emails received from a corporate remote office. The data portion is being

replaced by an attachment *.p7m . Which of the following factors are likely contributing to this issue?

- A. SMIME has been implemented between remote and central office MTAs.
- B. SMTPS has been implemented between remote and central office MTAs.
- C. The receiver MTA does not have the corresponding private key to decrypt the message.
- D. The receiver MTA does not have the corresponding public key to decrypt the message.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Which of the following antispam settings allows a FortiMail unit to scan all IP addresses in the headers of a received message?

- A. FortiGuard Antispam scan, Black IP scan
- B. Deep header scan, Black IP scan
- C. DNSBL scan
- D. SURBL scan

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

Which of the following is an advantage of using Banned Word scanning instead of Dictionary scanning?

- A. Mail Headers are inspected.
- B. It is easier to configure.
- C. Regular Expressions can be used.
- D. Non-ASCII characters are supported.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

Which operation is performed by the Forged IP scanning technique?

- A. DNS PTR record lookup on the sender's IP address then A record lookup on the canonical hostname
- B. DNS A record lookup on the sender's IP address then PTR record lookup
- C. DNS MX record lookup on the sender canonical hostname
- D. DNS TXT record lookup

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

How can a FortiMail administrator retrieve email account information from an LDAP Server instead of configuring this data manually on the unit?

- A. Configure the LDAP profile sections "User query options" and "Authentication" then associate the profile to the domain that is locally configured.
- B. Configure the LDAP profile sections "Authentication" and "User Alias Options" then associate the profile to the domain that is locally configured.
- C. Configure the LDAP profile sections "User query options" and "Authentication" and associate the profile to an incoming Recipient-based policy.
- D. This operation is not supported. The administrator has to configure the user email accounts manually.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

Which operational modes support High Availability?

- A. Transparent Mode
- B. Gateway Mode
- C. Server Mode

D. Config Mode

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Which of the following sentences is true regarding a Config Only cluster?

- A. Only two FortiMail units can join a Config Only cluster.
- B. The entire configuration file is synchronized between cluster members.
- C. Mail data and MTA queues are synchronized.
- D. A maximum of 25 FortiMail units can join a Config Only cluster.
- E. A Config Only cluster is generally deployed behind a Load Balancer.

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

Which SMTP sessions are defined as outgoing?

- A. All SMTP sessions received by the FortiMail units
- B. SMTP sessions for the protected domain
- C. SMTP messages destined for servers that are NOT protected domains
- D. All sessions generated from the internal network

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

Which of the following statements is true regarding oversized emails?

- A. The default maximum message size defined on the FortiMail unit is 10 MB.
- B. By default there is no maximum message size value defined on the FortiMail unit.
- C. The session profile parameter "Cap message size" can be used to increase the maximum message size.
- D. By default oversized emails are delivered at 0.00 local time.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

Which default Bayesian account can be used as the recipient address to train the spam database?

- A. learn-is-spam@localdomain
- B. learn-is-not-spam@localdomain
- C. is-spam@localdomain
- D. is-not-spam@localdomain

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

Which of the following features are available on a FortiMail unit operating in Server mode?

- A. Spam quarantine
- B. Content inspection
- C. Meeting Scheduling Assistant
- D. Botnet Snooping

Correct Answer: AB

Section: (none)

Explanation**Explanation/Reference:****QUESTION 43**

When using Sender Reputation on a FortiMail unit, which of the following actions can be taken against a source IP address generating spam or invalid email messages?

- A. Delay the email messages from that source IP address with a temporary fail.
- B. Reject the email messages from that source IP address with a permanent fail.
- C. Quarantine all the email messages from that source IP address.
- D. Limit the number of email messages allowed from that source IP address.

Correct Answer: ABD

Section: (none)

Explanation**Explanation/Reference:****QUESTION 44**

A FortiMail unit installed in Transparent mode protects a mail domain training1.lab on a mail server with IP address 172.16.1.1.

On the protected domain, the "Use this domain's SMTP server to deliver the mail" setting is ENABLED and the "Hide the transparent box" setting is DISABLED.

An email from userA@external.lab to user1@training1.lab (172.16.1.1) is intercepted by the FortiMail unit.

Which of the following statements is true based on this scenario?

- A. The FortiMail unit does its own MX Lookup to route the email to its destination.
- B. The FortiMail unit will act as a full transparent proxy between the client and the mail server with the IP address 172.16.1.1.
- C. The FortiMail unit will add a received header to the email message.
- D. The FortiMail unit will forward the email message using the original source IP address of the client.

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:**

QUESTION 45

Which of the following allow a TLS profile to be used?

- A. Access Control Receive Rule
- B. Access Control Delivery Rule
- C. IP-based policy
- D. Recipient-based policy

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Examine the SMTP session below to determine which of the following statements is TRUE:

```
220 server.internal.lab ESMTP Smtpd; Fri, 5 Mar 2010 10:15:17 +0100
ehlo 192.168.5.192
250-server.internal.lab Hello [192.168.5.192], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 10485760
250-DSN
250-AUTH LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250-STARTTLS
250-DELIVERBY
250 HELP
mail from: <user1@external.lab>
250 2.1.0 <user1@external.lab>... Sender ok
rcpt to: <user1@internal1.lab>
250 2.1.5 <user1@internal1.lab>... Recipient ok
data
354 Enter mail, end with "." on a line by itself
This is a test
.
250 2.0.0 o259FHGe000418-o259FHGf000418 Message accepted for delivery
quit
221 2.0.0 server.internal.lab closing connection
```

- A. The remote MTA FQDN is server.internal.lab.
- B. The remote MTA IP address is 192.168.5.192.
- C. The session has been unexpectedly closed by the sender MUA.
- D. The remote MTA does not support SMTP over TLS.
- E. The SMTP id is o259FHGe000418-o259FHGf000418.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

On a FortiMail unit operating in Transparent mode, which of the following parameters determines the direction of an SMTP session?

- A. The destination IP address
- B. The source IP address
- C. The recipient domain address
- D. The source domain address

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

Which CLI command was used to generate the output shown below:

```
Version: FortiMail-400B v4.0,build0103,091223 (GA Patch 1)
Virus-DB: 11.551(03/05/2010 01:02)
Serial-Number: FE400B3M09000140
BIOS version: 00010010
Log disk: Capacity 92 GB, Used 32 MB ( 0.04%), Free 92 GB
Mailbox disk: Capacity 371 GB, Used 277 MB ( 0.08%) , Free 370 GB
Hostname: server
Operation Mode: Server
HA configured mode: Off
HA effective mode: Off
```

Distribution: International
Branch point: 103
System time: Fri Mar 5 15:04:04 2010

- A. diag system top
- B. get sys performance
- C. get sys status
- D. diag netlink neighbor list

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Which History Log field indicates the action taken by the FortiMail unit regarding a specific email?

- A. Classified
- B. Disposition
- C. Resolved
- D. Type

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

An email message received by the FortiMail unit is subject to the Bounce Verification antispam check under which circumstances?

- A. The envelope MAIL FROM field contains a null reverse-path.
- B. Bounce Verification is enabled in the antispam profile.
- C. The recipient domain has a valid MX record.
- D. A Bounce Verification key is created and activated.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

Which of the following describe the functionality of the quarantine control account?

- A. It populates the envelope MAIL FROM field of the quarantine spam report.
- B. It populates the envelope RCPT TO field of the quarantine spam report.
- C. It can be used to submit spam emails.
- D. Email users can release quarantined emails by sending an email to this account.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

Which High Availability mode should an administrator choose to provide increased processing capabilities?

- A. Active-Passive
- B. Config-Only
- C. Load-Balance
- D. Standalone

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

In an LDAP query, which variable can be used to identify the full email address?

- A. \$u

- B. \$m
- C. \$g
- D. \$s

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

Which of the following statements regarding SMTPs and SMTP over TLS are true?

- A. SMTPS connections are initiated on port 465.
- B. SMTP over TLS connections are entirely encrypted and initiated on port 465.
- C. The command STARTTLS is used to initiate SMTP over TLS.
- D. In an SMTPS session, the identities of both sender and receiver are encrypted.
- E. In an SMTP over TLS session, the identities of both sender and receiver are encrypted.

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Which of the following antispam techniques is NOT part of the FortiGuard Antispam service?

- A. DNSBL
- B. SURBL
- C. SHASH
- D. BATV

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

Which of the following DNS records is commonly used to identify where to send mail for a particular domain name?

- A. MX record
- B. PTR record
- C. A record
- D. NS record

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

Which of the following profile types on a FortiMail unit make use of the system quarantine to isolate email messages?

- A. Content Monitor Profile
- B. Antispam Profile (Outgoing)
- C. Session Profile
- D. Antivirus Profile

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

Which of the following features can be used to hide internal email domains and email addresses?

- A. User Alias
- B. Address Map
- C. User Group
- D. Group Alias

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

Which of the following statements is true regarding an Active Passive HA configuration?

- A. Different hardware models can be used to form a cluster.
- B. The administrator can manage the slave unit only through the master unit.
- C. Units operating in Transparent mode cannot be used to form a cluster.
- D. The mail data and MTA queues can be synchronized between master and slave units.
- E. A maximum of two FortiMail units can be used to form a cluster.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

What is the outcome of the following CLI commands executed on a FortiMail unit operating in Transparent Mode?

```
config system interface
edit port1
set ip 192.168.1.20 255.255.255.0
set allowaccess http ping ssh
end
```

- A. The management IP address of the unit will be 192.168.1.20/24.
- B. The unit will accept HTTPS sessions on port1.
- C. The unit will accept Telnet sessions on port1.
- D. The unit will accept HTTP sessions on port1.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

What is the outcome of the following CLI commands executed on a FortiMail unit operating in Transparent mode?

```
config system interface
edit port2
set bridge-member disable
end
```

- A. Interface port2 is administratively down.
- B. Interface port2 is removed from the transparent bridge.
- C. Interface port2 is added to the transparent bridge.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

An administrator of a FortiMail unit operating in Server Mode has been given the requirement to configure disk quotas for all the users of a specific domain. How can the administrator achieve this requirement?

- A. Define a disk quota value in the User Preferences section.
- B. Define a disk quota value in the User section.
- C. Define a disk quota value under Protected domain > Advanced.
- D. Define a disk quota value in a Resource Profile.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

Which of the following situations could explain why an email message would be in the dead mail queue on a FortiMail unit operating in Gateway mode?

- A. The DNS server is not responding.
- B. The upstream Mail Transfer Agent (MTA) is performing Greylisting against the sender of the email message.
- C. The sender and the recipient addresses are invalid.
- D. There is a temporary network problem.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

Which operational mode allows the FortiMail unit to operate as a full featured mail server rather than just a mail relay agent?

- A. Server Mode
- B. Transparent Mode
- C. Gateway Mode
- D. High Availability Mode

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

Which of the following statements is true regarding Message Delivery Rules?

- A. They apply to incoming SMTP sessions.
- B. They apply to SMTP sessions initiated by the FortiMail unit.
- C. If the action is set to Discard the message is dropped.
- D. A TLS profile can be associated to the session.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

An SMTP client successfully authenticates with a FortiMail unit with no access list entries configured. Which of the following statements correctly describes the expected behavior of the FortiMail unit in this scenario?

- A. The FortiMail unit will relay all email messages from the authenticated client.
- B. The FortiMail unit will deny relaying the email message and will send an SMTP 550 error to the authenticated client.
- C. The FortiMail unit will only relay email messages from the authenticated client to recipients on the FortiMail unit's protected email domains.
- D. The FortiMail unit will discard all email messages from the authenticated client.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

Which of the following statements regarding SMTP Authentication is true?

- A. It can be enabled in Recipient-based policies only.
- B. It can be enabled in IP-based policies only.
- C. When enabled in Recipient or IP-based policies, it is supported but not enforced.
- D. It can be enforced through Access Control Rules only.

Correct Answer: CD

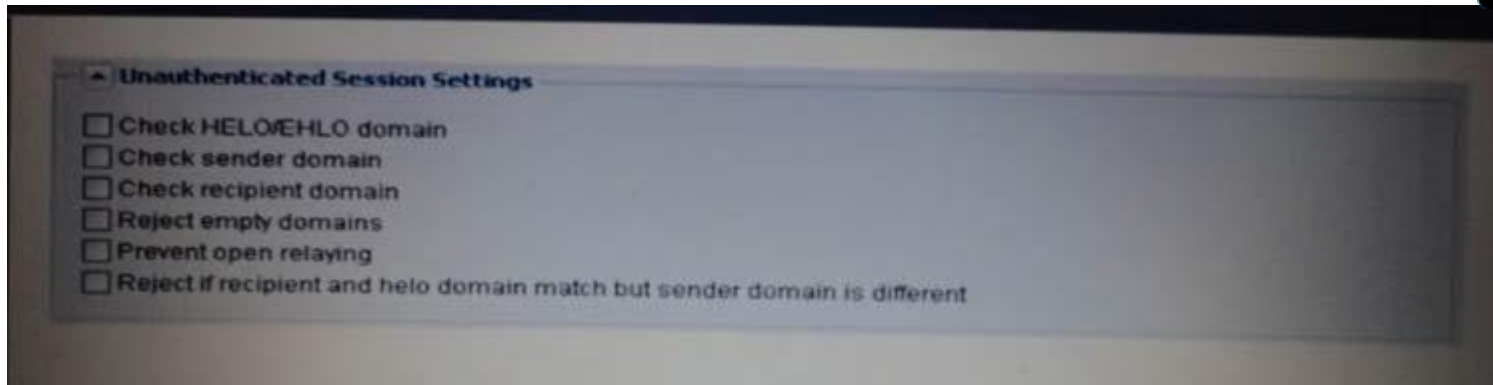
Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

The option Prevent open relaying is shown in the exhibit.



Which of the following statements is true regarding this option?

- A. Prevent open relaying is only available in Transparent mode.
- B. Prevent open relaying is only available in Server Mode.
- C. Prevent open relaying blocks all unauthenticated sessions.
- D. Prevent open relaying blocks all unencrypted sessions.

Correct Answer: AC

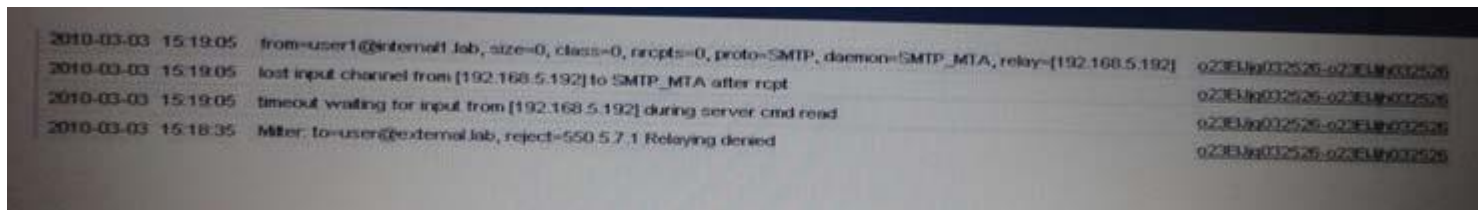
Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

Examine the event logs shown in the exhibit and determine which of the following statements is true:



- A. The sender user1@internal1.lab did not perform authentication.
- B. The recipient IP address is 192.168.5.192.

- C. The email is rejected because of Greylist scanning.
- D. The domain external.lab is not defined on the FortiMail unit.

Correct Answer: AD

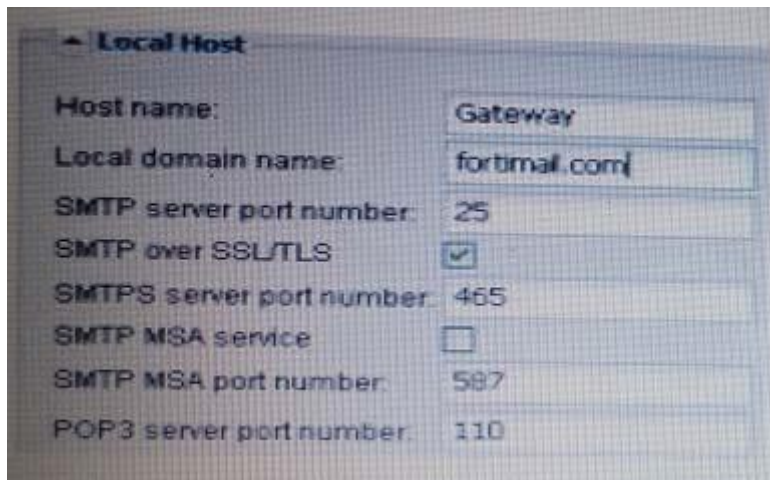
Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

The checkbox SMTP over SSL/TLS is enabled as indicated in the exhibit.



Which of the following statements is true regarding this scenario?

- A. SMTPS connections will be accepted by this FortiMail unit.
- B. SMTP over TLS connections will be accepted by this FortiMail unit.
- C. The FortiMail unit will use SMTP over SSL/TLS for all outgoing SMTP sessions.
- D. The FortiMail unit will use SMTP over SSL/TLS for all SMTP sessions initiated by the unit.

Correct Answer: AB

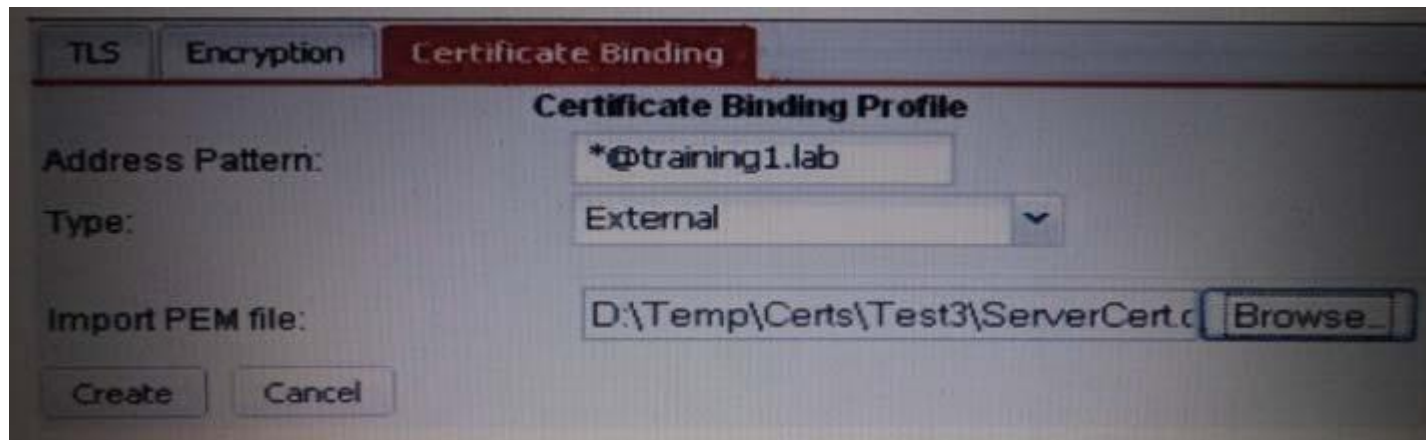
Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

What is the meaning of "Type External" in the Certificate Binding Profile shown in the exhibit?



- A. Emails generated from the FortiMail unit for domain training1.lab will be encrypted with the public key of the remote MTA.
- B. Emails received by the FortiMail unit for domain training1.lab will be decrypted.
- C. Emails received from the domain training1.lab will be decrypted by the FortiMail unit.
- D. The training1.lab domain is stored on an external MTA.

Correct Answer: A

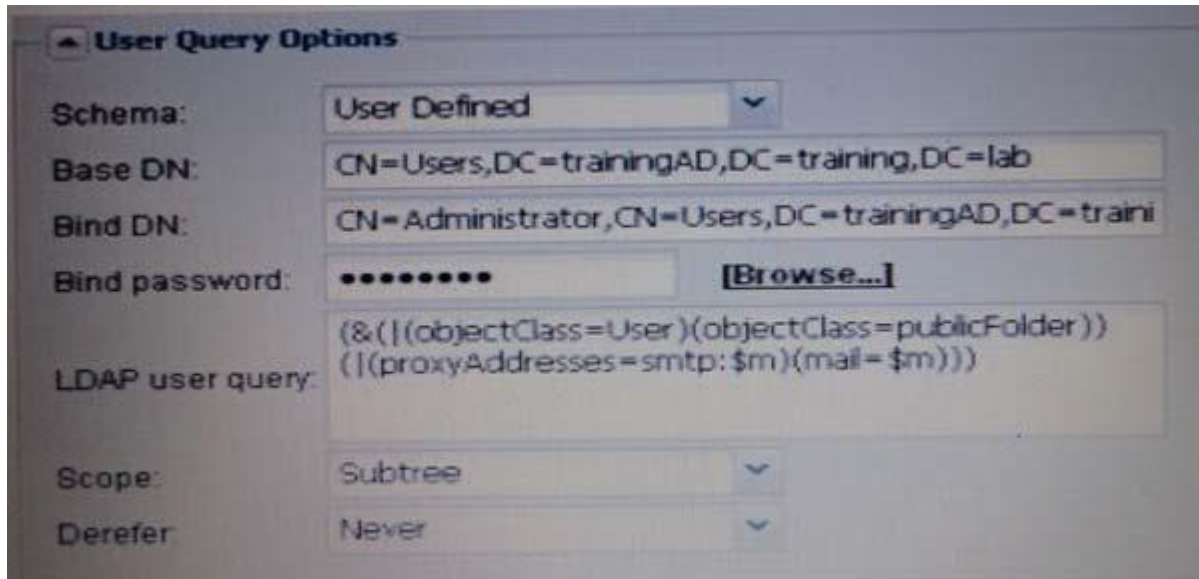
Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

In the exhibit, what does the field Base DN indicate?



User Query Options

Schema: User Defined

Base DN: CN=Users,DC=trainingAD,DC=training,DC=lab

Bind DN: CN=Administrator,CN=Users,DC=trainingAD,DC=traini

Bind password: [Browse...]

LDAP user query: (&(|(objectClass=User)(objectClass=publicFolder))(|(proxyAddresses=smtp:\$m)(mail=\$m)))

Scope: Subtree

Derefer: Never

- A. Distinguished name of the LDAP tree from within which the search is performed.
- B. Distinguished name of the LDAP user with enough rights to query the LDAP tree.
- C. The base DN determines how the user credentials must be entered in order for the search to be successful.
- D. LDAP query string.

Correct Answer: A

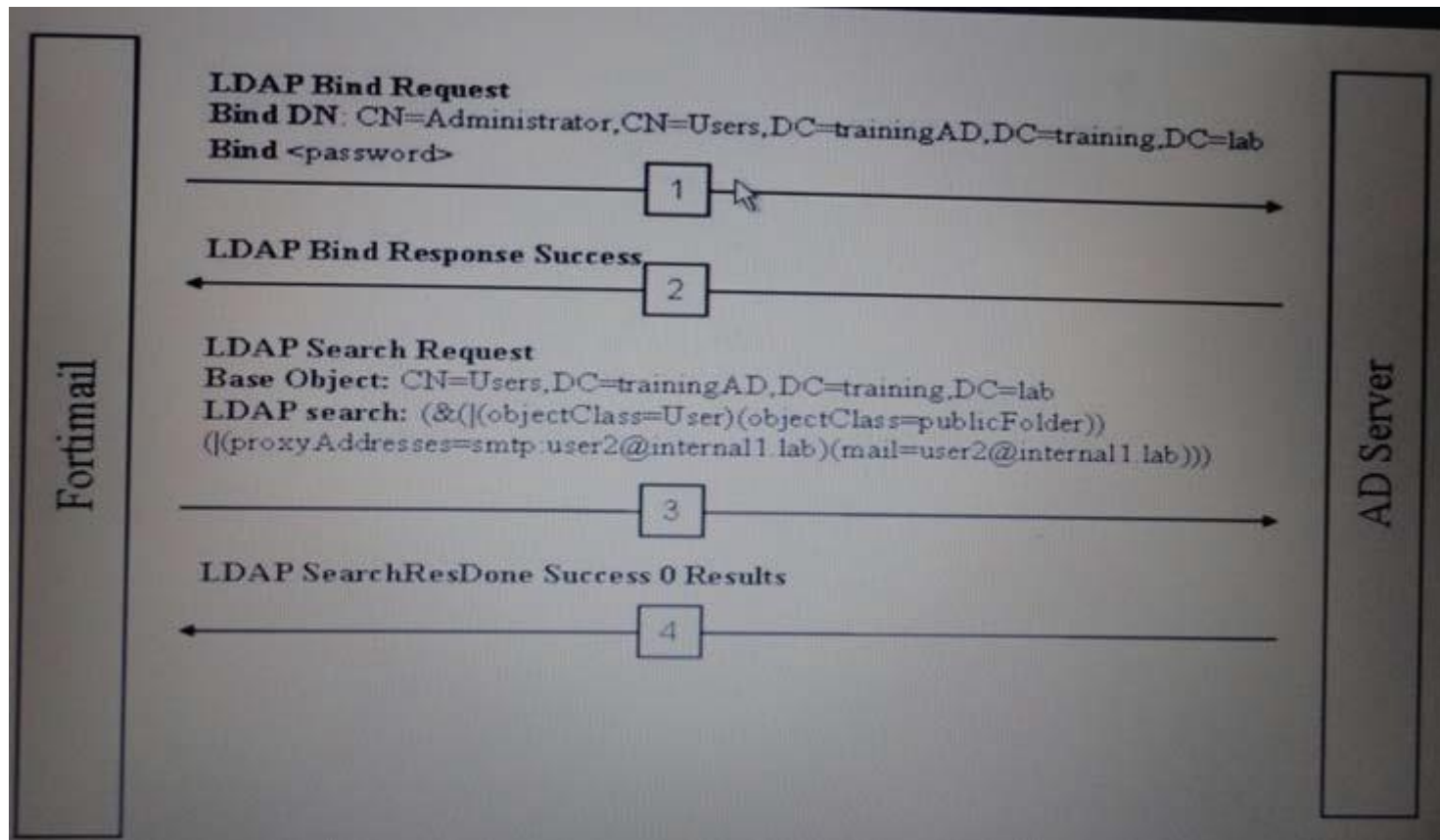
Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

A FortiMail administrator is investigating an LDAP issue in which the LDAP query is failing. The exhibit displays an extract of the messages being traced.



Why is the LDAP query failing?

- A. The Base Object in the search request should match the Bind DN in the bind request.
- B. The FortiMail unit is not authorized to search for users associated with domain internal1.lab.
- C. The LDAP lookup could not find any object whose attribute is matching email address user2@internal1.lab.
- D. The LDAP search query contained invalid parameters.

Correct Answer: C

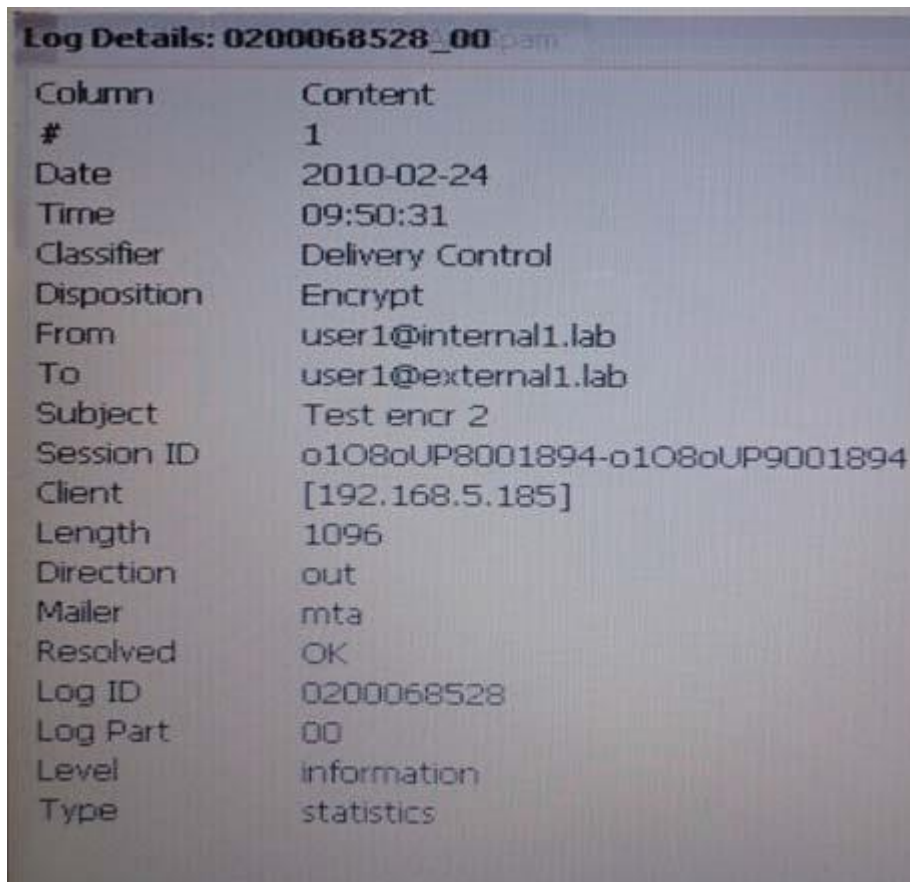
Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

Based upon the exhibit, which of the following statements are true?

A screenshot of a log entry titled "Log Details: 0200068528_00 pam". The log is presented as a table with two columns: "Column" and "Content".

Column	Content
#	1
Date	2010-02-24
Time	09:50:31
Classifier	Delivery Control
Disposition	Encrypt
From	user1@internal1.lab
To	user1@external1.lab
Subject	Test encr 2
Session ID	o1O8oUP8001894-o1O8oUP9001894
Client	[192.168.5.185]
Length	1096
Direction	out
Mailer	mta
Resolved	OK
Log ID	0200068528
Log Part	00
Level	information
Type	statistics

- A. The FortiMail unit received an encrypted email.
- B. The sender of the email is user1@external1.lab.
- C. The MIME content of the email has been encrypted by the FortiMail unit.
- D. The email is incoming.

Correct Answer: C

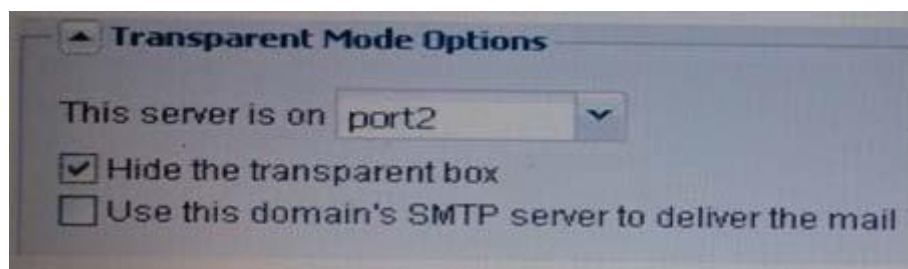
Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

Based upon the exhibit, which of the following statements are true?



- A. The new session initiated by the FortiMail proxy will reuse the sender IP.
- B. The FortiMail unit will add a received header to the email message.
- C. This option applies to outgoing SMTP sessions only.
- D. Email headers will not contain any reference to the FortiMail transparent device.

Correct Answer: AD

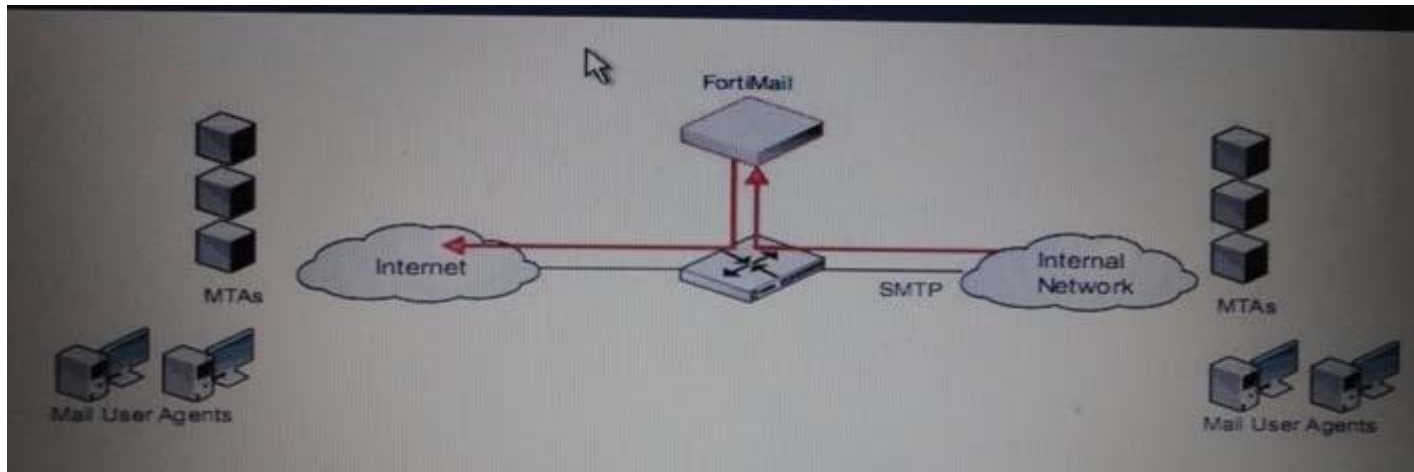
Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

Consider the diagram shown in the exhibit.



The FortiMail unit is operating in Transparent Mode and the administrator wishes to perform transparent inspection on all SMTP sessions.

How can this requirement be achieved?

- A. Configure one interface of the FortiMail unit in route mode.
- B. Redirect SMTP sessions to the Transparent mode FortiMail unit using Policy Based Routing on the router.
- C. Configure the Transparent mode FortiMail unit to only inspect POP3 sessions.
- D. The configuration required is not supported in Transparent mode.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

Which protection profile can be used to protect against Directory Harvest attacks?

- A. authentication profile
- B. session profile
- C. dictionary profile
- D. security profile

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

Examining the History Log shown in the exhibit,

Exhibit is Missing (Exhibit shows sessions were aborted because session limit reached -> delayed)

determine the best possible explanation for these log entries?

- A. Some of the mail message fields were missing -- clear evidence that the mail messages were crafted by Spammers seeking to avoid detection.
- B. These sessions were aborted prior to the mail connection being established.
- C. The mail traffic was encrypted.
- D. Under heavy load, the FortiMail unit may not log all parameters.

Correct Answer: B

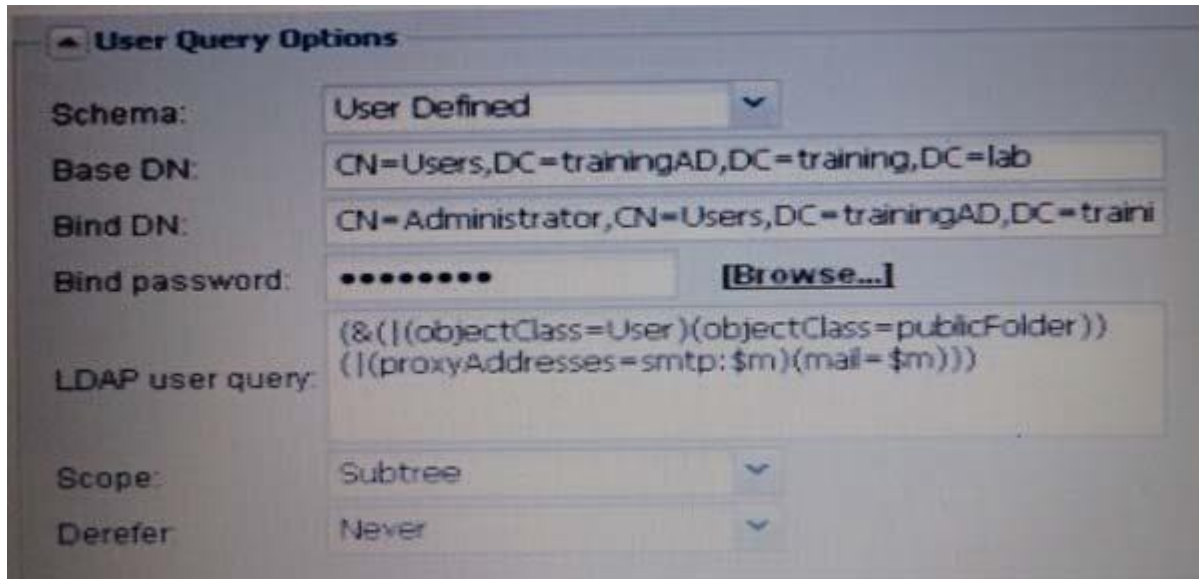
Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

In the exhibit,



User Query Options

Schema: User Defined

Base DN: CN=Users,DC=trainingAD,DC=training,DC=lab

Bind DN: CN=Administrator,CN=Users,DC=trainingAD,DC=traini

Bind password: [Browse...]

LDAP user query: (&(|(objectClass=User)(objectClass=publicFolder))(|(proxyAddresses=smtp:\$m)(mail=\$m)))

Scope: Subtree

Derefer: Never

which LDAP attributes contain the email address parameter?

- A. ObjectClass
- B. proxyAddresses
- C. mail
- D. none of the above

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

Consider the proxy configuration shown in the exhibit.

Exhibit is Missing (Exhibit shows SMTP traffic is allowed on port 1)

A FortiMail unit is configured to protect the domain internal1.lab 192.168.11.101.
All emails from IP 192.168.5.1/32 are relayed through an Access Control Rule.
An SMTP session from 192.168.5.1 to 192.168.11.102 (internal2.lab) is received on port1.

Which statement best describes how the FortiMail unit will handle the SMTP session?

- A. The SMTP session will be handled by the incoming proxy.
- B. The SMTP session will be bridged without inspection.
- C. The SMTP session will be inspected.
- D. The SMTP session will be relayed to the IP 192.168.11.102.
- E. The SMTP session will be rejected.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

When inspecting and delivering mail messages, which of the following steps could be taken by a FortiMail unit operating in Transparent mode?

- A. Inspect for viruses.
- B. Inspect content of the message payload.
- C. Inspect for spam.
- D. Perform a routing lookup to decide the next hop MTA.

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference: