

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 1

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 2

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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

The screenshot shows the 'AntiVirus Action Profile' configuration page in FortiMail. The 'Action' tab is selected. The configuration includes:

- Domain: internal.lab
- Profile name: AC_Action
- Direction: Incoming
- Tag email's subject line: With value:
- Insert new header: With value:
- Deliver to alternate host:
- BCC: [BCC](#)
- Replace infected/suspicious body or attachment(s):
- Notify with profile: --None--
- Reject: --None--
- Discard:
- System quarantine to folder: --None--
- 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

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 3

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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: @

Recipient Pattern

Type: @

Profiles

Authentication and Access

Authentication type:

Authentication profile:

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

Show Suggested Answer



Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 4

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

FortiMail is configured with the protected domain "example.com". Identify which of the following envelope addresses will require an access receive rule to relay 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: accounts@example.com RCPT TO: sales@external.org
- D. MAIL FROM: support@example.com RCPT TO: marketing@example.com

Show Suggested Answer



Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 5

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 6

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 7

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the FortMail mail server settings shown in the exhibit; then answer the question below.

Mail Server Settings	Relay Host List	Disclaimer	Disclaimer Exclusion List
Local Host Local Host Setting			
Host name:	<input type="text" value="mx"/>		
Local domain name:	<input type="text" value="example.com"/>		
SMTP server port number:	<input type="text" value="25"/>		
SMTP over SSL/TLS	<input checked="" type="checkbox"/>		
SMTPS server port number:	<input type="text" value="465"/>		
SMTP MSA service	<input checked="" type="checkbox"/>		
SMTP MSA port number:	<input type="text" value="587"/>		
POP3 server port number:	<input type="text" value="110"/>		
Default domain for authentication:	<input type="text" value="--None--"/>		
Webmail access	<input checked="" type="checkbox"/> Redirect HTTP to HTTPS		

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

- A. mx.example.com will enforce SMTPS on all outbound sessions
- B. mx.example.com will display STARTTLS as one of the supported commands in SMTP sessions
- C. mx.example.com will accept SMTPS connections
- D. mx.example.com will drop any inbound plaintext SMTP connection

Show Suggested Answer

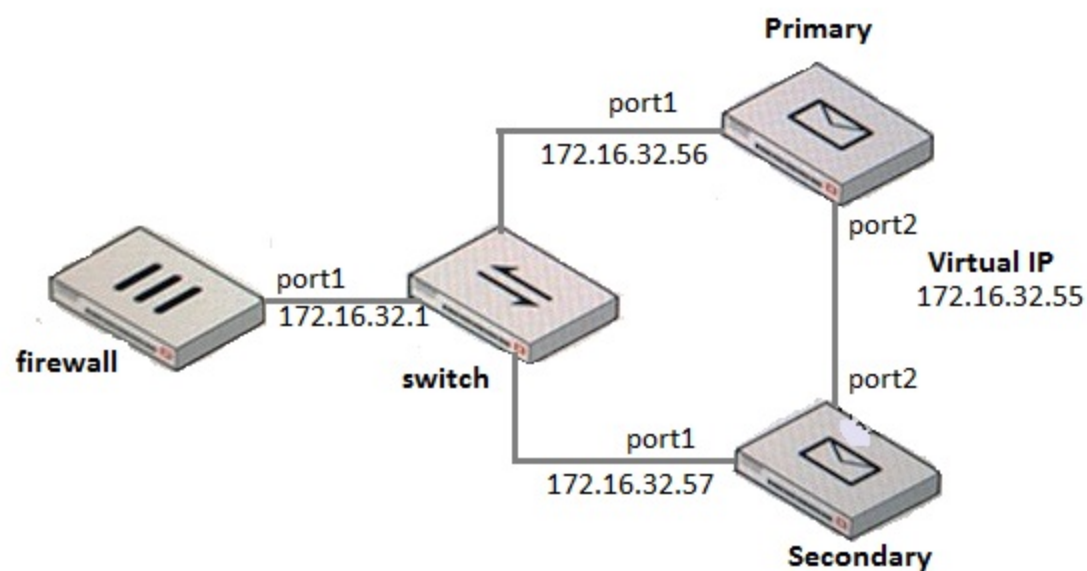
Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 8

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the FortiMail active-passive cluster shown in the exhibit; then answer the question below.



Primary HA Interface Configuration

HA Interface

Port:	port1...
Enable port monitor	<input type="checkbox"/>
Heartbeat status:	Disable
Peer IP address:	0.0.0.0
Peer IPv6 address:	::
Virtual IP action:	Ignore
Virtual IP address:	0.0.0.0 / 0
Virtual IPv6 address:	:: / 0

Which of the following parameters are recommended for the Primary FortiMail's HA interface configuration? (Choose three.)

- A. Enable port monitor: disable
- B. Peer IP address: 172.16.32.57
- C. Heartbeat status: Primary
- D. Virtual IP address: 172.16.32.55/24
- E. Virtual IP action: Use

Show Suggested Answer





Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 9

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 10

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the FortiMail IBE users shown in the exhibit; then answer the question below



The screenshot shows the FortiMail IBE user management interface. At the top, there are tabs for 'Active User', 'Expired User', 'Secure Question', 'IBE Authentication', and 'IBE Domain'. Below the tabs are buttons for 'Delete', 'Maintenance', and 'Reset User'. The main area displays a table of users with the following columns: Enabled, Email, First Name, Last Name, Status, Creation Time, and Last Access. The table contains two rows of data.

Enabled	Email	First Name	Last Name	Status	Creation Time	Last Access
<input checked="" type="checkbox"/>	hjordan@external.com	Hal	Jordan	Activated	Wed, 12 Apr 2017 13:00:28 EDT	Wed, 12 Apr 2017 13:01:25 EDT
<input checked="" type="checkbox"/>	krayner@external.com			Pre-registered	Wed, 12 Apr 2017 13:02:13 EDT	Wed, 12 Apr 2017 13:02:13 EDT

Which one of the following statements describes the Pre-registered status of the IBE user krayner@external.com?

- A. The user was registered by an administrator in anticipation of IBE participation
- B. The user has completed the IBE registration process but has not yet accessed their IBE email
- C. The user has received an IBE notification email, but has not accessed the HTTPS URL or attachment yet
- D. The user account has been de-activated, and the user must register again the next time they receive an IBE email

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 11

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/>	

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

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 12

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Which of the following statements are true regarding FortiMail's behavior when using the built-in MTA to process email in transparent mode? (Choose two.)

- A. FortiMail can queue undeliverable messages and generate DSNs
- B. If you disable the built-in MTA, FortiMail will use its transparent proxies to deliver email
- C. FortiMail ignores the destination set by the sender and uses its own MX record lookup to deliver email
- D. MUAs need to be configured to connect to the built-in MTA to send email

Show Suggested Answer

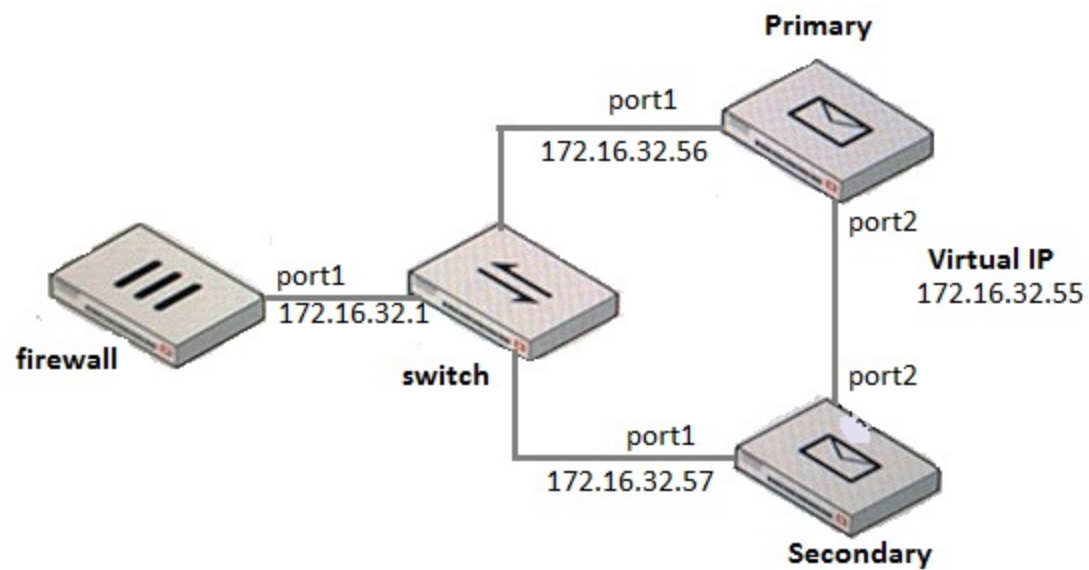


Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 13

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)



What IP address should the DNS MX record for this deployment resolve to?

- A. 172.16.32.1
- B. 172.16.32.57
- C. 172.16.32.55
- D. 172.16.32.56

Show Suggested Answer

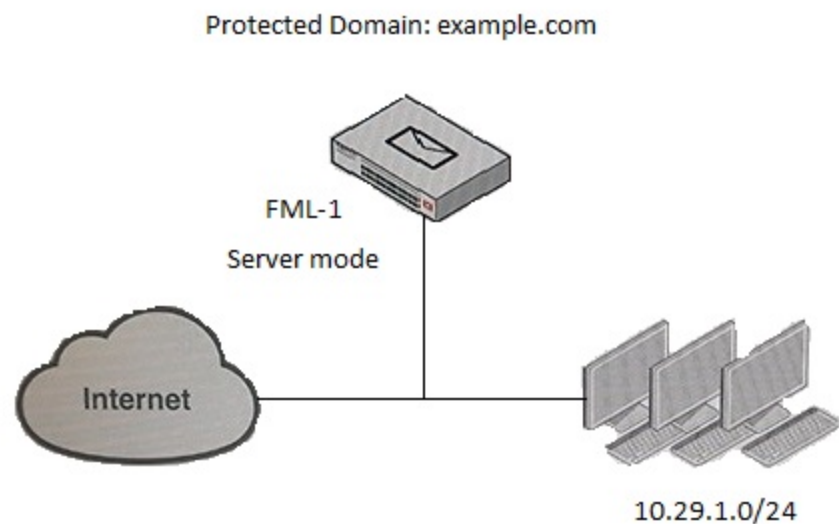
Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 14

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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



FortiMail

Access Control Rule

Enabled

Sender pattern: Regular expression

Recipient pattern: Regular expression

Sender IP/netmask: /

Reverse DNS pattern: Regular expression

Authentication status:

TLS profile:

Action:

Comments:

An administrator must enforce authentication on FML-1 for all outbound email from the example.com domain. Which of the following settings should be used to configure the access receive rule? (Choose two.)

- A. The Sender IP/netmask should be set to 10.29.1.0/24
- B. The Authentication status should be set to Authenticated
- C. The Recipient pattern should be set to *@example.com
- D. The Action should be set to Reject

[Show Suggested Answer](#)

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 15

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the configured routes shown in the exhibit; then answer the question below.

```
#get sys route
= = [1]
destination: 0.0.0.0/0          gateway:10.47.1.1    interface: port1
= = [2]
destination: 10.1.100.0/22     gateway:10.38.1.1    interface: port3
= = [3]
destination: 10.1.100.0/24     gateway:10.29.1.1    interface: port2
= = [4]
destination: 10.1.100.0/24     gateway:10.10.1.1    interface: port4

Number of items: 4
```

Which interface will FortiMail use to forward an email message destined for 10.1.100.252?

- A. port2
- B. port4
- C. port3
- D. port1

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 16

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the FortiMail IBE service configuration shown in the exhibit; then answer the question below.

IBE Encryption

Enable IBE service	<input checked="" type="checkbox"/>
IBE service name:	<input type="text" value="Example Secure Portal"/>
User registration expiry time (days):	<input type="text" value="30"/>
User inactivity expiry time (days):	<input type="text" value="90"/>
Encrypted email storage expiry time (days):	<input type="text" value="180"/>
Password reset expiry time (hours):	<input type="text" value="24"/>
Allow secure replying	<input checked="" type="checkbox"/>
Allow secure forwarding	<input type="checkbox"/>
Allow secure composing	<input type="checkbox"/>
IBE base URL:	<input type="text"/>
"Help" content URL:	<input type="text" value="-"/>
"About" content URL:	<input type="text"/>
Allow custom user control	<input type="checkbox"/>

Which of the following statements describes the User inactivity expiry time of 90 days?

- A. First time IBE users must register to access their email within 90 days of receiving the notification email message
- B. After initial registration, IBE users can access the secure portal without authenticating again for 90 days
- C. Registered IBE users have 90 days from the time they receive a notification email message to access their IBE email
- D. IBE user accounts will expire after 90 days of inactivity, and must register again to access new IBE email message

Show Suggested Answer

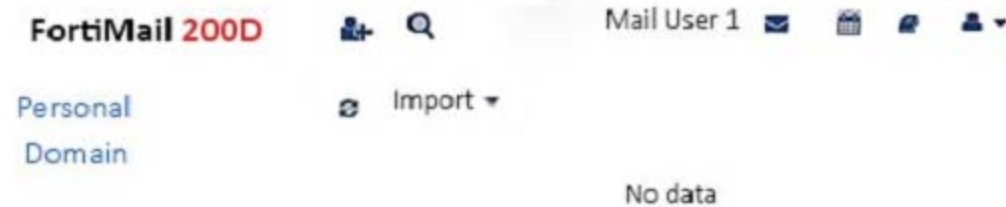
Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 17

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the FortiMail user webmail interface shown in the exhibit; then answer the question below.



Which one of the following statements is true regarding this server mode FortiMail's configuration?

- A. The protected domain-level service settings have been modified to allow access to the domain address book
- B. This user's account has a customized access profile applied that allows access to the personal address book
- C. The administrator has not made any changes to the default address book access privileges
- D. The administrator has configured an inbound recipient policy with a customized resource profile

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 18

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

A FortiMail administrator is investigating a sudden increase in DSNs being delivered to the protected domain for undeliverable email messages. After searching the logs, the administrator identifies that the DSNs were not generated as a result of any outbound email sent from the protected domain. Which FortiMail antispam technique can the administrator use to prevent this scenario? (Choose one.)

- A. Bounce address tag validation
- B. Spam outbreak protection
- C. Spoofed header detection
- D. FortiGuard IP Reputation

Show Suggested Answer



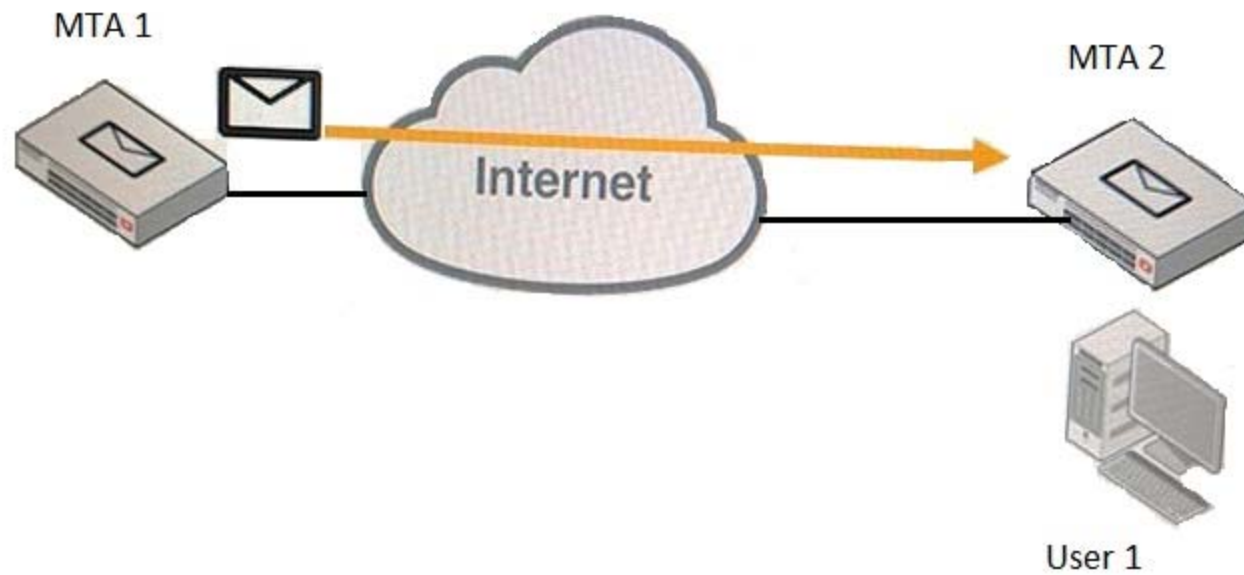
Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 19

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

Examine the exhibit; then answer the question below.



MTA 1 is delivering an email intended for User 1 to MTA 2. Which of the following statements about protocol usage between the devices are true? (Choose two.)

- A. MTA 2 will use IMAP to receive the email message from MTA 1
- B. MTA 1 will use SMTP to deliver the email message to MTA 2
- C. User 1 will use IMAP to download the email message from MTA 2
- D. MTA 1 will use POP3 to deliver the email message to User 1 directly

Show Suggested Answer

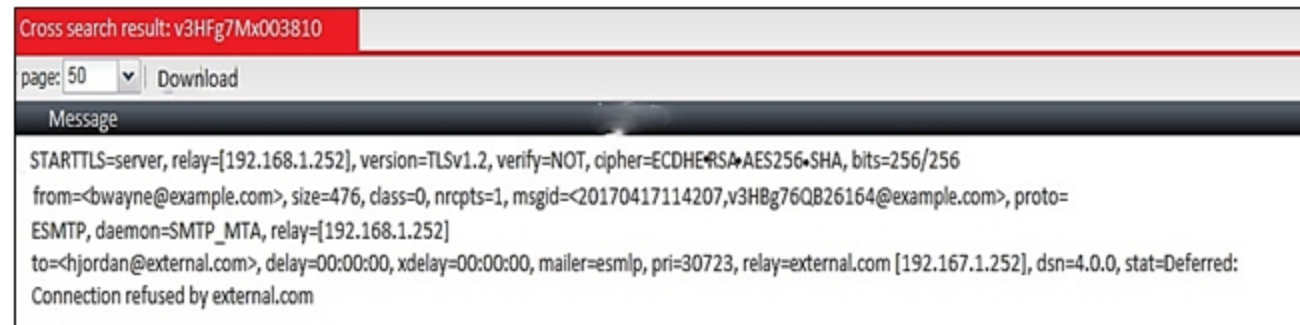
Actual exam question from Fortinet's NSE6_FML-5.3.8

Question #: 20

Topic #: 1

[\[All NSE6_FML-5.3.8 Questions\]](#)

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



Cross search result: v3HFg7Mx003810

page: 50 | Download

Message

```
STARTTLS=server, relay=[192.168.1.252], version=TLSv1.2, verify=NOT, cipher=ECDHE+RSA+AES256+SHA, bits=256/256
from=<bwayne@example.com>, size=476, class=0, nrpts=1, msgid=<20170417114207,v3HBg76QB26164@example.com>, proto=
ESMTP, daemon=SMTP_MTA, relay=[192.168.1.252]
to=<hjordan@external.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmlp, pri=30723, relay=external.com [192.167.1.252], dsn=4.0.0, stat=Deferred:
Connection refused by external.com
```

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

Show Suggested Answer