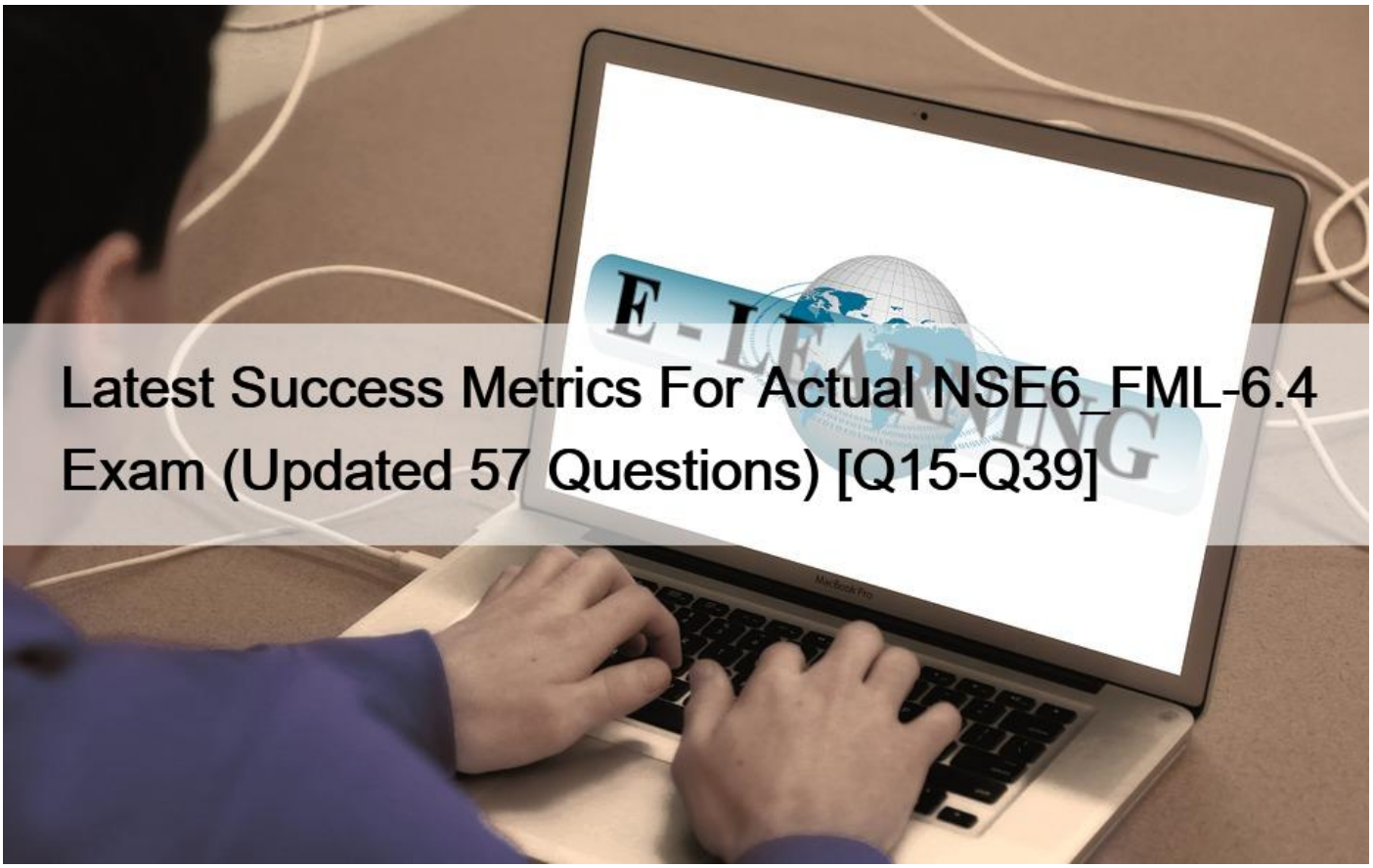
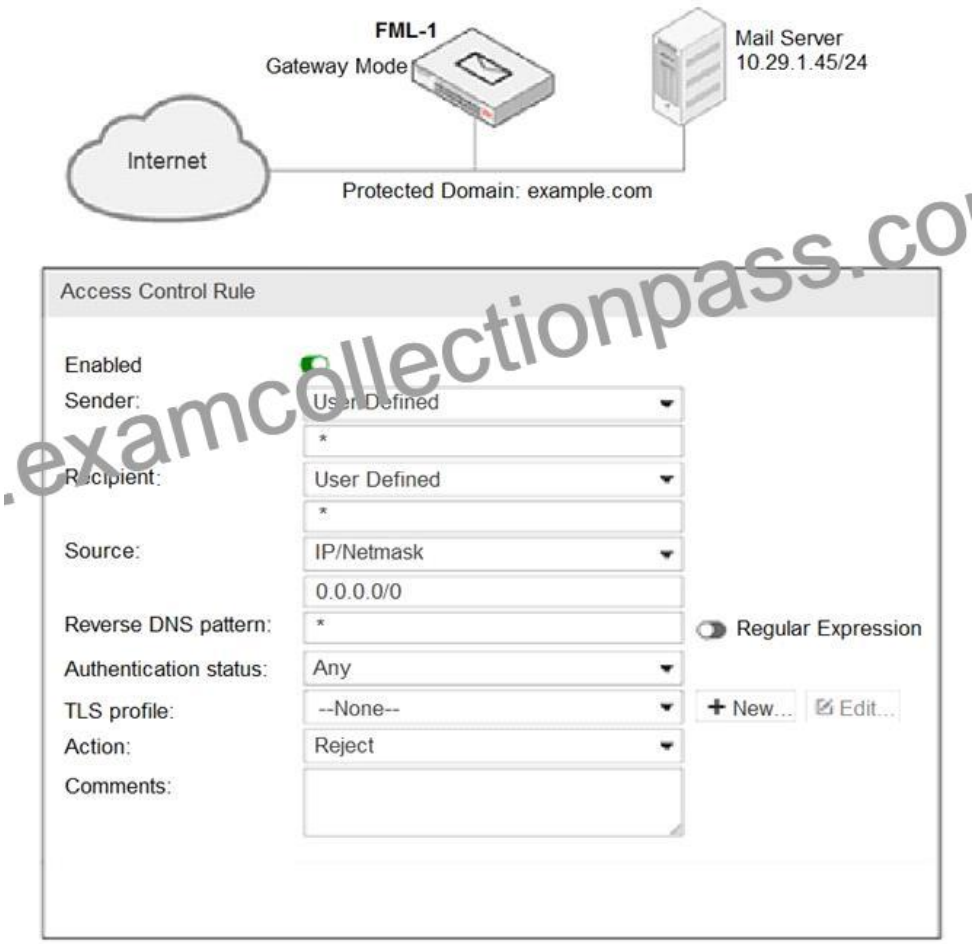
Latest Success Metrics For Actual NSE6_FML-6.4 Exam (Updated 57 Questions) [Q15-Q39



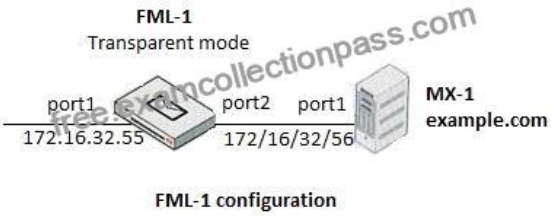
Latest Success Metrics For Actual NSE6_FML-6.4 Exam (Updated 57 Questions) Genuine NSE6_FML-6.4 Exam Dumps Free Demo Valid QA's NO.15 Refer to the exhibit.



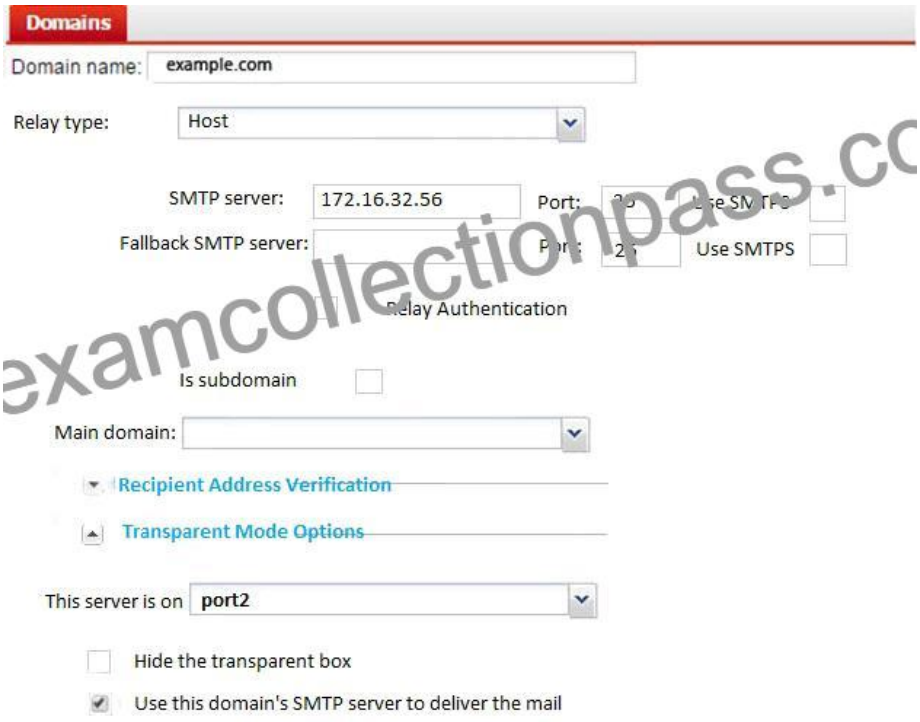
It is recommended that you configure which three access receive settings to allow outbound email from the example.com domain on FML-1? (Choose three.)

* The Sender pattern should be set to *@example.com
* The Action should be set to Relay
* The Recipient pattern should be set to 10.29.1.45/24
* The Enable check box should be cleared
* The Sender IP/netmask should be set to 10.29.1.45/32

NO.16 Refer to the exhibit.



FML-1 configuration



Which of the following statements are true regarding the transparent mode FortiMail’s email routing for the example.com domain? (Choose two.)

* FML-1 will use the built-in MTA for outgoing sessions
* FML-1 will use the transparent proxy for incoming sessions
* If incoming email are undeliverable, FML-1 can queue them to retry again later
* If outgoing email messages are undeliverable, FML-1 can queue them to retry later

NO.17 While testing outbound MTA functionality, an administrator discovers that all outbound email is being processed using policy IDs 1:2:0.

Which two reasons explain why the last policy ID value is 0? (Choose two.)

* Outbound email is being rejected
* IP policy ID 2 has the exclusive flag set
* There are no outgoing recipient policies configured
* There are no access delivery rules configured for outbound email

NO.18 Which two antispam techniques query FortiGuard for rating information? (Choose two.)

* DNSBL
* SURBL
* IP reputation
* URI filter

NO.19 Refer to the exhibit.

Which two message types will trigger this DLP scan rule? (Choose two.)
* An email message with a subject that contains the term “credit card” will trigger this scan rule
* An email that contains credit card numbers in the body, attachment, and subject will trigger this scan rule
* An email message that contains credit card numbers in the body will trigger this scan rule
* An email sent from sales@internal.lab will trigger this scan rule, even without matching any conditions

NO.20 An organization has different groups of users with different needs in email functionality, such as address book access, mobile device access, email retention periods, and disk quotas.

Which FortiMail feature specific to server mode can be used to accomplish this?
* Access profiles
* Address book management options
* Resource profiles

* Domain-level service settings

NO.21 What three configuration steps are required to enable DKIM signing for outbound messages on FortiMail? (Choose three.)
* Generate a public/private key pair in the protected domain configuration
* Enable DKIM check in a matching session profile
* Enable DKIM check in a matching antispam profile
* Publish the public key as a TXT record in a public DNS server
* Enable DKIM signing for outgoing messages in a matching session profile

NO.22 What are the configuration steps to enable DKIM signing for outbound messages on FortiMail? (Choose three.)
* Enable DKIM signing for outgoing messages in a matching session profile
* Publish the public key as a TXT record in a public DNS server
* Enable DKIM check in a matching session profile
* Enable DKIM check in a matching antispam profile
* Generate a public/private key pair in the protected domain configuration

DKIM Signing for Outbound Email

* To configure DKIM signing for outgoing messages, you must first generate a public and private key pair for the domain

* DKIM signatures are domain specific

* FortiMail generates and stores the private key, and uses it to generate the DKIM signature

– Download the public key and publish to your external DNS server

– Enable sign outgoing messages with a DKIM signature

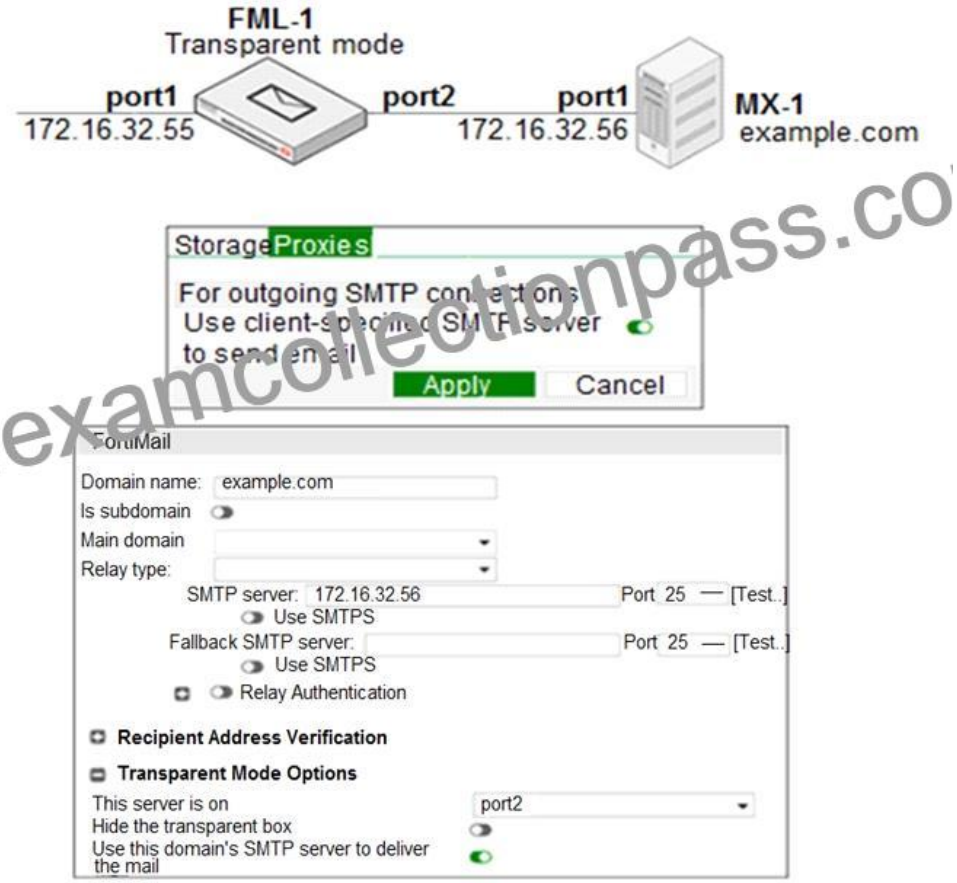
NO.23 Examine the configured routes shown in the exhibit; then answer the question below.

```
#get sys route
= = [1]
destination: 0.0.0.0/0          gateway:10.0.1.1      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?
* port2
* port4
* port3
* port1

NO.24 Refer to the exhibit.



Which two statements about how the transparent mode FortiMail device routes email for the example.com domain are true? (Choose two.)

* If incoming email messages are undeliverable, FML-1 can queue them to retry later
* If outgoing email messages are undeliverable, FM-1 can queue them to retry later
* FML-1 will use the built-in MTA for outgoing sessions
* FML-1 will use the transparent proxy for incoming sessions

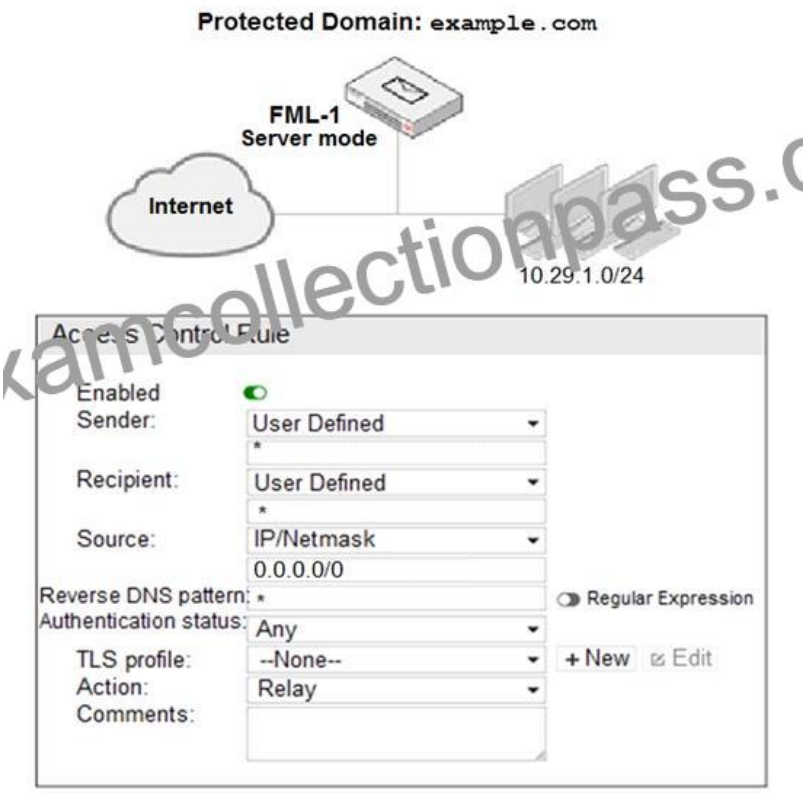
NO.25 Which firmware upgrade method for an active-passive HA cluster ensures service outage is minimal, and there are no unnecessary failovers?

* Break the cluster, upgrade the units independently, and then form the cluster
* Upgrade both units at the same time
* Upgrade the standby unit, and then upgrade the active unit
* Upgrade the active unit, which will upgrade the standby unit automatically

NO.26 Which two CLI commands, if executed, will erase all data on the log disk partition? (Choose two.)

* execute formatmaildisk
* execute formatmaildisk_backup
* execute formatlogdisk
* execute partitionlogdisk 40

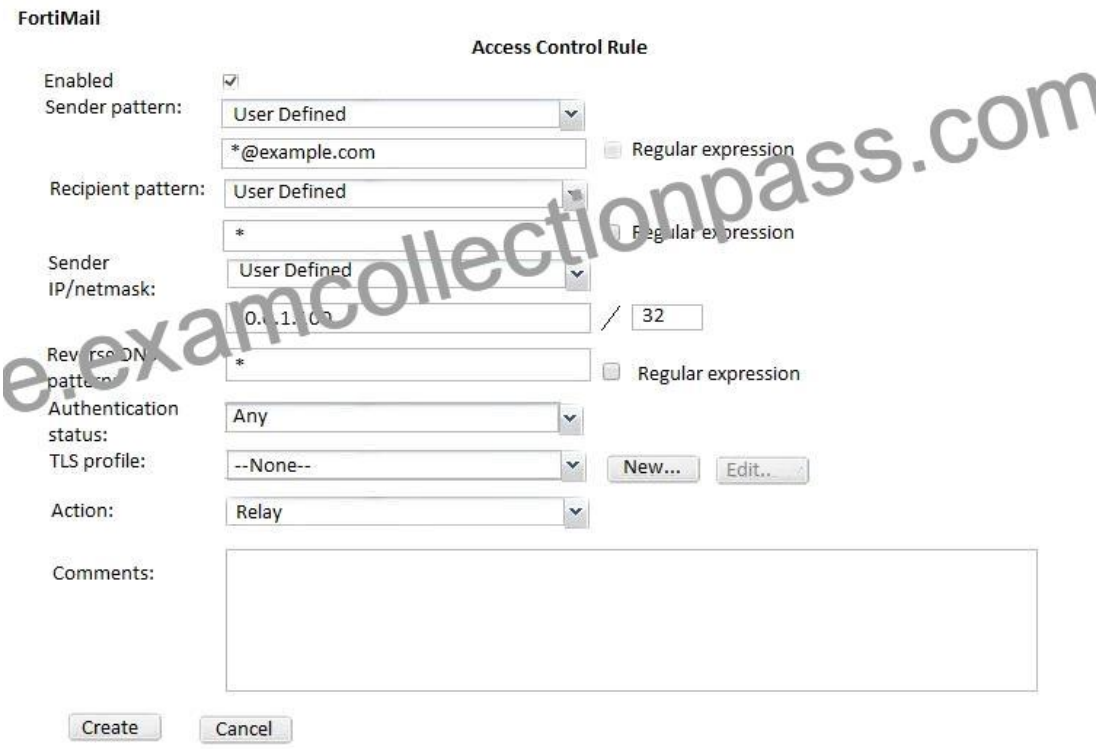
NO.27 Refer to the exhibit.



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

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

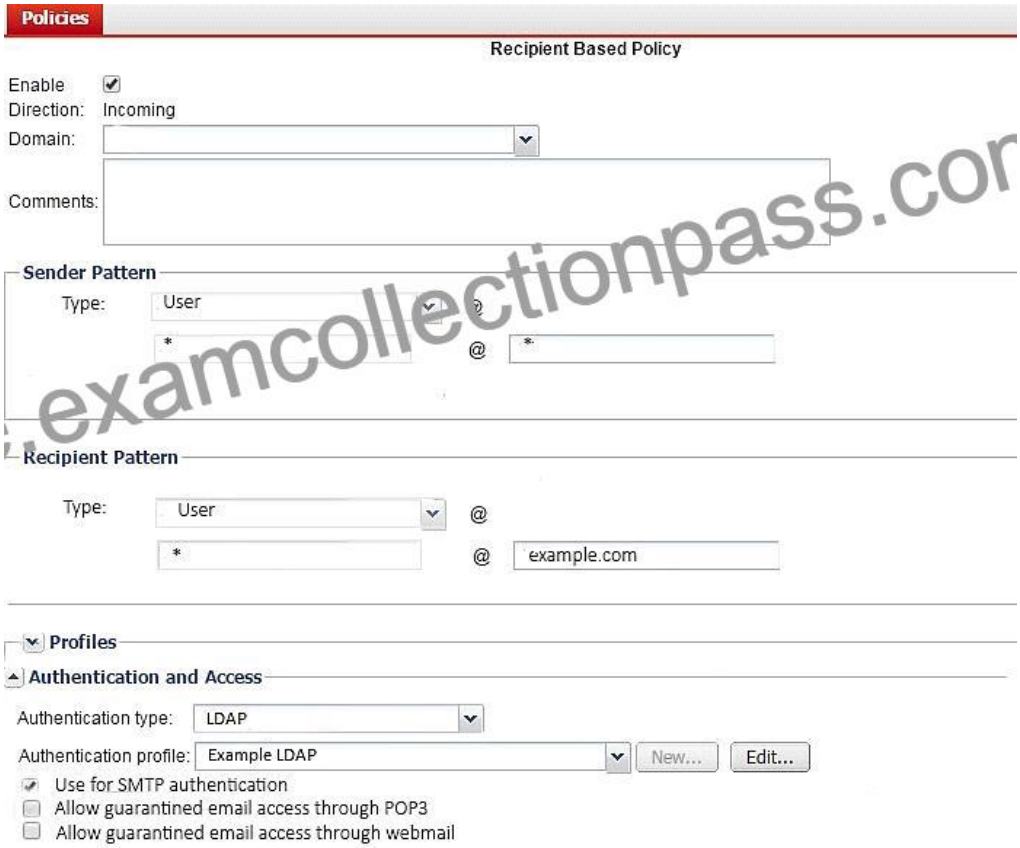
NO.28 Examine the access receive rule shown in the exhibit; then answer the question below.



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

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

NO.29 Examine the FortiMail recipient-based policy shown in the exhibit; then answer the question below.



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?

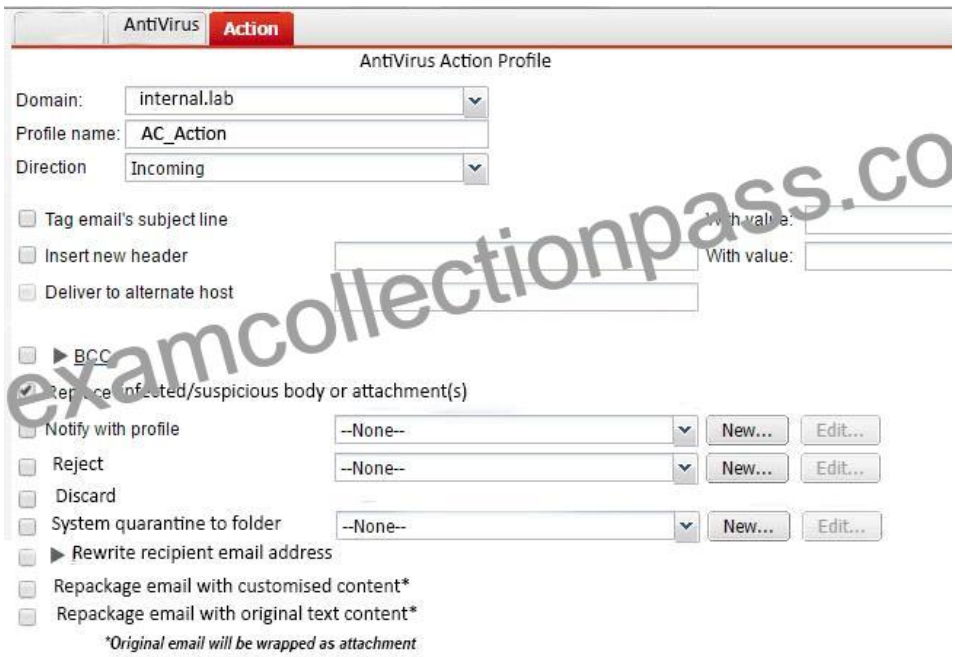
* Configure a matching IP policy with SMTP authentication and exclusive flag enabled
* Move the recipient policy to the top of the list
* Configure an access receive rule to verify authentication status
* Configure an access delivery rule to enforce authentication

NO.30 While reviewing logs, an administrator discovers that an incoming email was processed using policy IDs 0:4:9.

Which two scenarios will generate this policy ID? (Choose two.)

* Email was processed using IP policy ID 4
* Incoming recipient policy ID 9 has the exclusive flag set
* FortiMail applies the default behavior for relaying inbound email
* FortiMail configuration is missing an access delivery rule

NO.31 Examine the FortiMail antivirus action profile shown in the exhibit; then answer the question below.



What is the expected outcome if FortiMail applies this action profile to an email? (Choose two.)
* The sanitized email will be sent to the recipient’s personal quarantine
* A replacement message will be added to the email
* Virus content will be removed from the email
* The administrator will be notified of the virus detection

NO.32 Refer to the exhibit.

MTA-1 is delivering an email intended for User 1 to MTA-2.

Which two statements about protocol usage between the devices are true? (Choose two.)
* User 1 will use logs were generated load the email message from MTA-2
* MTA-2 will use IMAP to receive the email message from MTA-1
* MTA-1 will use POP3 to deliver the email message to User 1 directly

* MTA-1 will use SMTP to deliver the email message to MTA-2

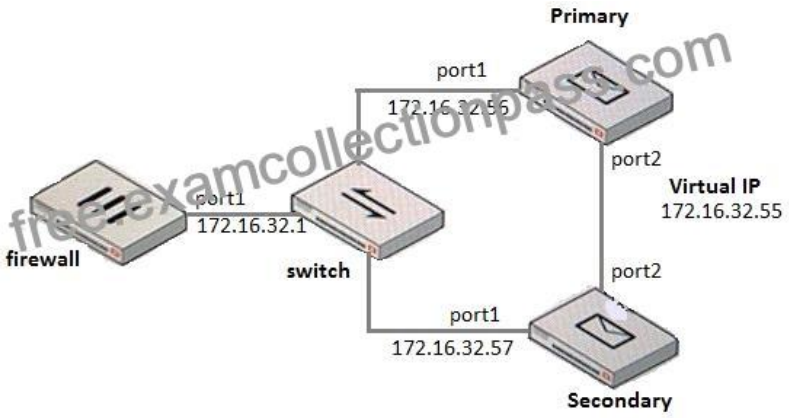
NO.33 Which of the following statements are true regarding FortiMail’s behavior when using the built-in MTA to process email in transparent mode? (Choose two.)
* FortiMail can queue undeliverable messages and generate DSNs
* If you disable the built-in MTA, FortiMail will use its transparent proxies to deliver email
* FortiMail ignores the destination set by the sender and uses its own MX record lookup to deliver email
* MUAs need to be configured to connect to the built-in MTA to send email

NO.34 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.)
* The FortiMail is experiencing issues delivering the email to the back-end mail server
* The logs were generated by a server mode FortiMail
* The logs were generated by a gateway or transparent mode FortiMail
* The FortiMail is experiencing issues accepting the connection from the remote sender

NO.35 Which three statements about SMTPS and SMTP over TLS are true? (Choose three.)
* SMTP over TLS connections are entirely encrypted and initiated on port 465
* SMTPS encrypts the identities of both the sender and receiver
* The STARTTLS command is used to initiate SMTP over TLS
* SMTPS encrypts only the body of the email message
* SMTPS connections are initiated on port 465

NO.36 Refer to the exhibit.



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

* 172.16.32.1
* 172.16.32.57
* 172.16.32.55
* 172.16.32.56