QUESTION 71
A network administrator is modifying an outgoing mail policy to enable domain protection for the organization. A DNS entry is created that has the public key.
Which two headers will be used as matching criteria in the outgoing mail policy? (Choose two.)

A. message-ID
B. sender
C. URL reputation
D. from
E. mail-from

Answer: BD

QUESTION 72
To comply with a recent audit, an engineer must configure anti-virus message handling options on the incoming mail policies to attach warnings to the subject of an email.
What should be configured to meet this requirement for known viral emails?

A. Virus Infected Messages
B. Unscannable Messages
C. Encrypted Messages
D. Positively Identified Messages

Answer: C

QUESTION 73
An administrator is managing multiple Cisco ESA devices and wants to view the quarantine emails from all devices in a central location.
How is this accomplished?

A. Disable the VOF feature before sending SPAM to the external quarantine.
B. Configure a mail policy to determine whether the message is sent to the local or external quarantine.
C. Disable the local quarantine before sending SPAM to the external quarantine.
D. Configure a user policy to determine whether the message is sent to the local or external quarantine.

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100000.html#task _1749146

QUESTION 74
A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy.
What is the reason of this?

A. The Tram* header is checked against all policies in a top-down fashion.
B. The message header with the highest priority is checked against each policy in a top-down fashion.
C. The To" header is checked against all policies in a top-down fashion.
D. The message header with the highest priority is checked against the Default policy in a top-down fashion.

Answer: D

QUESTION 75
An administrator identifies that, over the past week, the Cisco ESA is receiving many emails from certain senders and domains which are being consistently quarantined. The administrator wants to ensure that these senders and domain are unable to send anymore emails.
Which feature on Cisco ESA should be used to achieve this?

A. incoming mail policies
B. safelist
C. blocklist
D. S/MIME Sending Profile

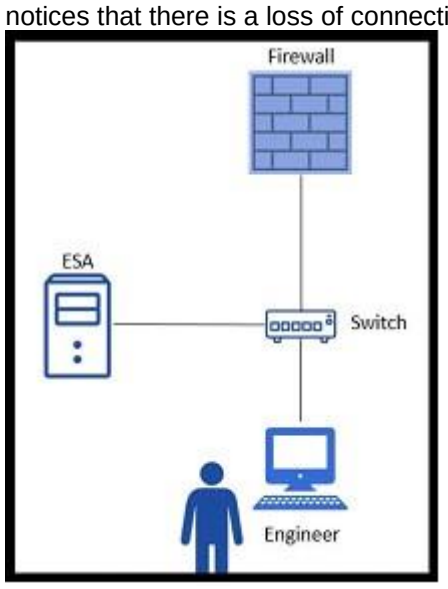
Answer: A

QUESTION 76
An engineer is testing mail flow on a new Cisco ESA and notices that messages for domain abc.com are stuck in the delivery queue. Upon further investigation, the engineer notices that the messages pending delivery are destined for 192.168.1.11, when they should instead be routed to 192.168.1.10.
What configuration change needed to address this issue?

A. Add an address list for domain abc.com.
B. Modify Destination Controls entry for the domain abc.com.
C. Modify the SMTP route for the domain and change the IP address to 192.168.1.10.
D. Modify the Routing Tables and add a route for IP address to 192.168.1.10.

Answer: C
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html

QUESTION 77
Refer to the exhibit. An engineer is trying to connect to a Cisco ESA using SSH and has been unsuccessful. Upon further inspection, the engineer notices that there is a loss of connectivity to the neighboring switch.

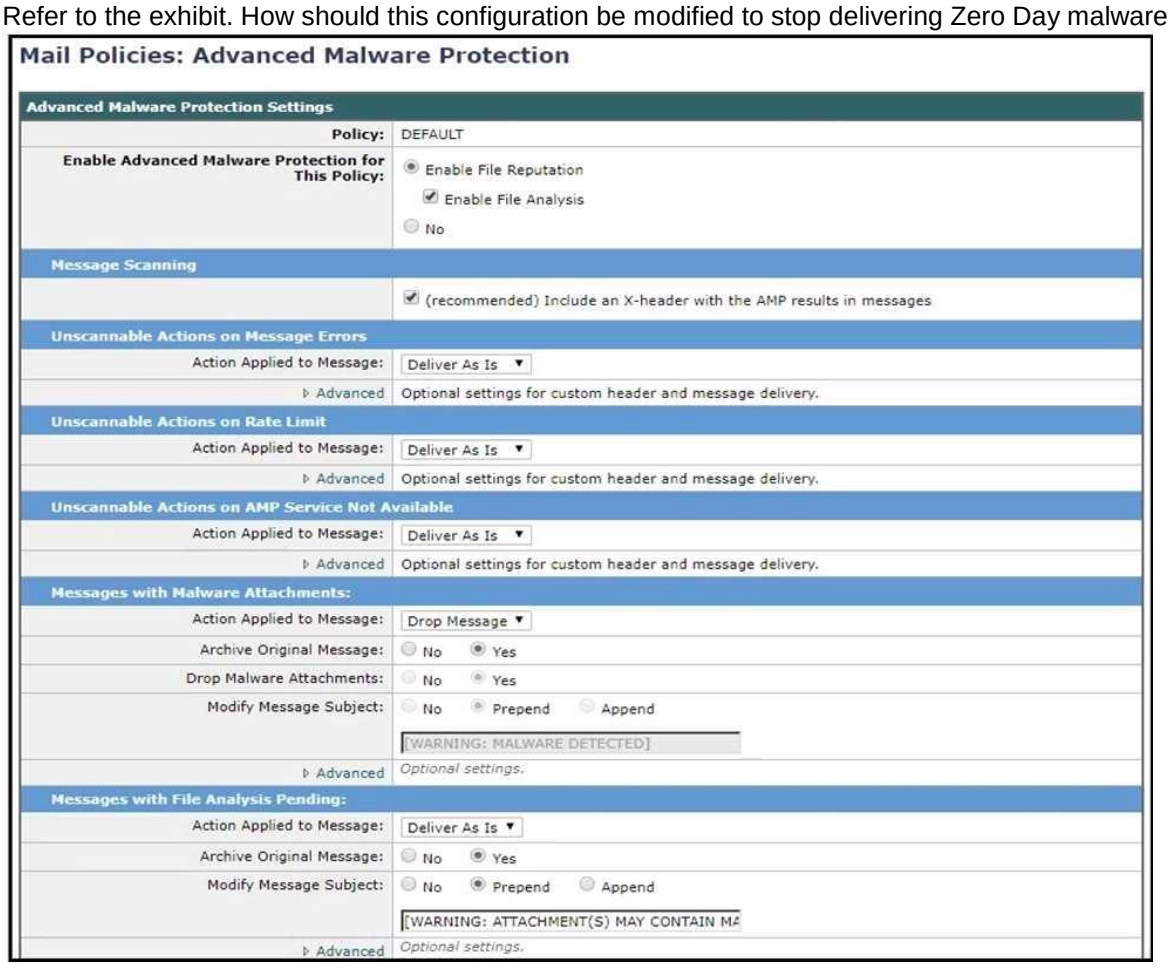


Which connection method should be used to determine the configuration issue?

A. Telnet
B. HTTPS
C. Ethernet
D. serial

Answer: D

QUESTION 78
Refer to the exhibit. How should this configuration be modified to stop delivering Zero Day malware attacks?



A. Change Unscannable Action from Deliver As Is to Quarantine.
B. Change File Analysis Pending action from Deliver As Is to Quarantine.
C. Configure mailbox auto-remediation.
D. Apply Prepend on Modify Message Subject under Malware Attachments.

Answer: C

QUESTION 79
Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?

A. Set up the interface group with the flag.
B. Issue the altsrchost command.
C. Map the envelope sender address to the host.

D. Apply a filter on the message.

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01000.html#con_1133810

QUESTION 80
A Cisco ESA administrator was notified that a user was not receiving emails from a specific domain. After reviewing the mail logs, the sender had a negative sender-based reputation score.
What should the administrator do to allow inbound email from that specific domain?

A. Create a new inbound mail policy with a message filter that overrides Talos.
B. Ask the user to add the sender to the email application's allow list.
C. Modify the firewall to allow emails from the domain.
D. Add the domain into the allow list.

Answer: D

QUESTION 81
An email containing a URL passes through the Cisco ESA that has content filtering disabled for all mail policies. The sender is sampleuser@test1.com, the recipients are testuser1@test2.com, testuser2@test2.com, testuser3@test2.com, and mailer1@test2.com. The subject of the email is Test Document395898847. An administrator wants to add a policy to ensure that the Cisco ESA evaluates the web reputation score before permitting this email.
Which two criteria must be used by the administrator to achieve this? (Choose two.)

A. Subject contains Test Document"
B. Sender matches test1.com
C. Email body contains a URL
D. Date and time of email
E. Email does not match mailer1@test2.com

Answer: AC

QUESTION 82
A recent engine update was pulled down for graymail and has caused the service to start crashing. It is critical to fix this as quickly as possible.
What must be done to address this issue?

A. Roll back to a previous version of the engine from the Services Overview page.
B. Roll back to a previous version of the engine from the System Health page.
C. Download another update from the IMS and Graymail page.
D. Download another update from the Service Updates page.

Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_0100010.html#task_9F07A032042F48C6AEDB69D325CD3C5F

QUESTION 83
Refer to the exhibit. An engineer needs to change the existing Forged Email Detection message filter so that it references a newly created dictionary named `Executives'.

```
TEST: if (forged-email-detection ("support", 60)) { fed("from", ""); }
```

What should be done to accomplish this task?

A. Change "from" to "Executives".
B. Change "TESF to "Executives".
C. Change fed' to "Executives".
D. Change "support" to "Executives".

Answer: D

QUESTION 84
An administrator has created a content filter to quarantine all messages that result in an SPF hardfail to review the messages and determine whether a trusted partner has accidentally misconfigured the DNS settings. The administrator sets the policy quarantine to release the messages after 24 hours, allowing time to review while not interrupting business.
Which additional option should be used to help the end users be aware of the elevated risk of interacting with these messages?

A. Notify Recipient
B. Strip Attachments
C. Notify Sender
D. Modify Subject

Answer: D

QUESTION 85
A company has deployed a new mandate that requires all emails sent externally from the Sales Department to be scanned by DLP for PCI-DSS compliance. A new DLP policy has been created on the Cisco ESA and needs to be assigned to a mail policy named `Sales' that has yet to be created.
Which mail policy should be created to accomplish this task?

A. Outgoing Mail Policy
B. Preliminary Mail Policy
C. Incoming Mail Flow Policy
D. Outgoing Mail Flow Policy

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html#task_14094

QUESTION 86
Spreadsheets containing credit card numbers are being allowed to bypass the Cisco ESA.
Which outgoing mail policy feature should be configured to catch this content before it leaves the network?

A. file reputation filtering
B. outbreak filtering
C. data loss prevention
D. file analysis

Answer: B