300-720Q&As

Securing Email with Cisco Email Security Appliance (SESA)

Pass Cisco 300-720 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/300-720.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which action is a valid fallback when a client certificate is unavailable during SMTP authentication on Cisco ESA?

A. LDAP Query

B. SMTP AUTH

C. SMTP TLS

D. LDAP BIND

Correct Answer: B

Reference: 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_011011.html

QUESTION 2

An engineer is tasked with reviewing mail logs to confirm that messages sent from domain abc.com are passing SPF verification and being accepted by the Cisco ESA. The engineer notices that SPF verification is not being performed and that SPF is not being referenced in the logs for messages sent from domain abc.com.

Why is the verification not working properly?

A. SPF verification is disabled in the Recipient Access Table.

B. SPF verification is disabled on the Mail Flow Policy.

C. The SPF conformance level is set to SIDF compatible on the Mail Flow Policy.

D. An SPF verification Content Filter has not been created.

Correct Answer: D

QUESTION 3

A list of company executives is routinely being spoofed, which puts the company at risk of malicious email attacks. An administrator must ensure that executive messages are originating from legitimate sending addresses. Which two steps must be taken to accomplish this task? (Choose two.)

A. Create an incoming content filter with SPF detection.

B. Create a content dictionary including a list of the names that are being spoofed.

C. Enable the Forged Email Detection feature under Security Settings.

D. Enable DMARC feature under Mail Policies.

E. Create an incoming content filter with the Forged Email Detection condition.

Correct Answer: AD

QUESTION 4

When DKIM signing is configured, which DNS record must be updated to load the DKIM public signing key?

A. AAAA record

B. PTR record

C. TXT record

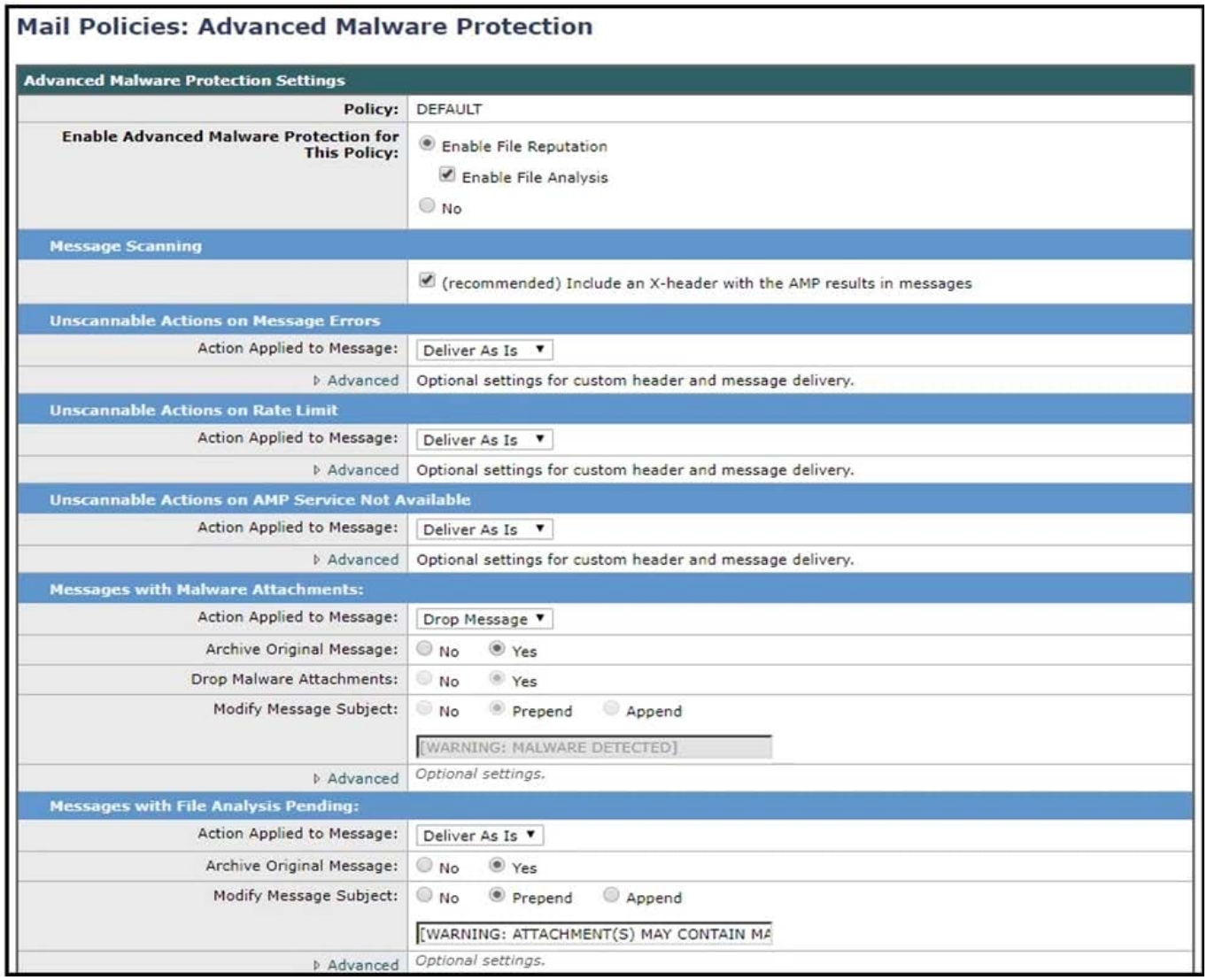
D. MX record

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa-configure-dkim-signing.html

QUESTION 5

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.

Correct Answer: C