300-720^{Q&As}

300-720^{Q&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.geekcert.com/300-720.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which SMTP extension does Cisco ESA support for email security?

A. ETRN

B. UTF8SMTP

C. PIPELINING

D. STARTTLS

Correct Answer: D

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_011000.html

QUESTION 2

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 3

How does the graymail safe unsubscribe feature function?

A. It strips the malicious content of the URI before unsubscribing.

B. It checks the URI reputation and category and allows the content filter to take an action on it.

C. It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.

D. It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200383-Graymail-Detection-and-Safe-Unsubscribin.html

QUESTION 4

An administrator manipulated the subnet mask but was still unable to access the user interface. How must the administrator access the appliance to perform the initial configuration?

A. Use the data 2 port.

B. Use the serial or console port.

C. Use the data 1 port.

D. Use the management port.

Correct Answer: B

QUESTION 5

A remote financial institution is implementing email encryption. It is required that all inbound emails use SMTP over TLS. What must be done to accomplish this?

A. Disable TLS certificates.

B. Utilize Cisco Registered Envelope Service.

C. Leverage Cisco Talos Threat Intelligence Group.

D. Enable Application Inspection and Control for SMTP.

Correct Answer: D