



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 benefit does enabling external spam quarantine on Cisco SMA provide?

- A. ability to back up spam quarantine from multiple Cisco ESAs to one central console
- B. access to the spam quarantine interface on which a user can release, duplicate, or delete
- C. ability to scan messages by using two engines to increase a catch rate
- D. ability to consolidate spam quarantine data from multiple Cisco ESA to one central console

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-0/user_guide/b_SMA_Admin_Guide/b_SMA_Admin_Guide_chapter_010101.html

QUESTION 2

An administrator needs to configure a Cisco ESA to verify that a specific mail server is authorized to send emails for a domain. To reduce overhead, the administrator does not want SSL type encryption or decryption to be used in this process. What must be configured on the Cisco ESA to meet this requirement?

- A. DomainKeys Identified Mail
- B. PKI signing keys
- C. Asymmetric keys
- D. Sender Policy Framework

Correct Answer: D

QUESTION 3

An engineer must limit responses from the gateway that are directed to invalid email addresses. How should the LDAP server be configured to accomplish this goal?

- A. Validate the sender email address via an LDAP query during the SMTP conversation.
- B. Validate the sender email address via SMTP Call-Ahead to query an external SMTP server.
- C. Limit the number of invalid recipients per sender to stop responses after crossing the threshold.
- D. Limit the number of invalid responses per recipient to stop responses after crossing the threshold.

Correct Answer: D

QUESTION 4



DRAG DROP

Drag and drop the SMTP Call-Ahead Server Profile Settings from the left onto the descriptions on the right.

Select and Place:

| | |
|----------------------------|--|
| interface | action to be taken when a recipient validation request temporarily fails |
| MAIL FROM | address to be used for the SMTP conversation with the SMTP server |
| validation failure action | used to initiate the SMTP conversation with the SMTP server |
| temporary failure action | number of seconds to wait for a result from the SMTP server |
| validation request timeout | action to be taken when a recipient validation request fails |

Correct Answer:

| | |
|--|----------------------------|
| | temporary failure action |
| | MAIL FROM |
| | interface |
| | validation request timeout |
| | validation failure action |

QUESTION 5

Which two statements about configuring message filters within the Cisco ESA are true? (Choose two.)



- A. The filters command executed from the CLI is used to configure the message filters.
- B. Message filters configuration within the web user interface is located within Incoming Content Filters.
- C. The filterconfig command executed from the CLI is used to configure message filters.
- D. Message filters can be configured only from the CLI.
- E. Message filters can be configured only from the web user interface.

Correct Answer: AD

Reference: <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213940-esa-using-a-message-filter-to-take-act.html>

[Latest 300-720 Dumps](#)

[300-720 PDF Dumps](#)

[300-720 Braindumps](#)