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:

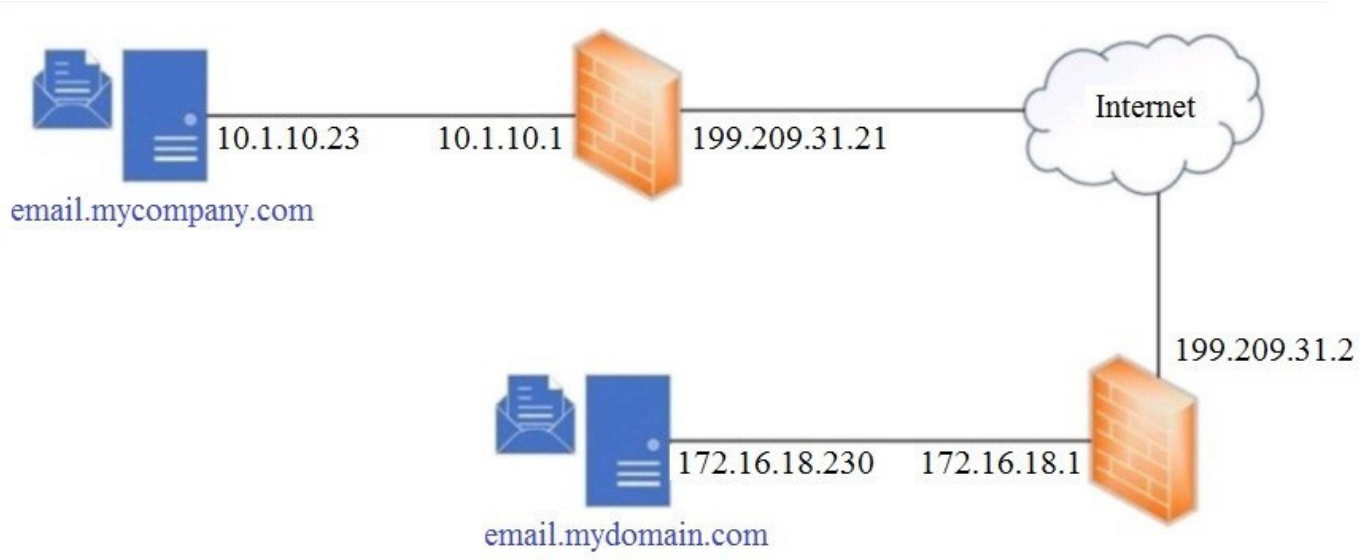
https://www.leads4pass.com/300-720.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.



Which SPF record is valid for mycompany.com?

A. v=spf1 a mx ip4:199.209.31.2 -all

B. v=spf1 a mx ip4:10.1.10.23 -all

C. v=spf1 a mx ip4:199.209.31.21 -all

D. v=spf1 a mx ip4:172.16.18.230 -all

Correct Answer: D

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 tries to implement phishing simulations to test end users, but they are being blocked by the Cisco ESA. Which two components, when added to the allow list, allow these simulations to bypass antispam scanning? (Choose two.)

A. receivers

B. domains

C. reputation score

D. spf check

E. senders

Correct Answer: CE

QUESTION 4

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

Correct Answer: A

QUESTION 5

An organization wants to use its existing Cisco ESA to host a new domain and enforce a separate corporate policy for that domain.

What should be done on the Cisco ESA to achieve this?

A. Use the smtproutes command to configure a SMTP route for the new domain.

B. Use the deliveryconfig command to configure mail delivery for the new domain.

C. Use the dsestconf command to add a separate destination for the new domain.

D. Use the altrchost command to add a separate gateway for the new domain.

Correct Answer: A

QUESTION 6

An engineer is configuring a Cisco ESA for the first time and needs to ensure that any email traffic coming from the internal SMTP servers is relayed out through the Cisco ESA and is tied to the Outgoing Mail Policies. Which Mail Flow Policy setting should be modified to accomplish this goal?

A. Exception List

B. Connection Behavior

C. Bounce Detection Signing

D. Reverse Connection Verification

Correct Answer: B

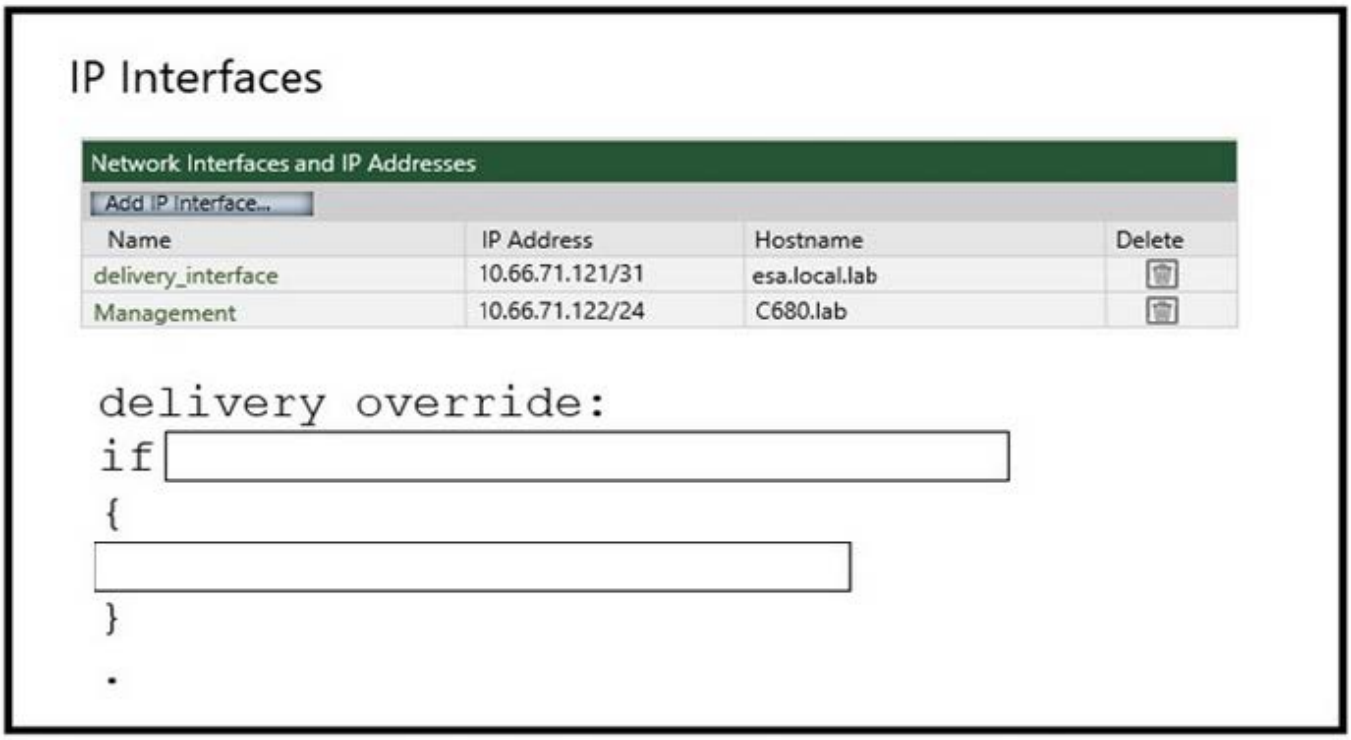
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html

QUESTION 7

DRAG DROP

An administrator must ensure that emails sent from cisco_123@externally.com are routed through an alternate virtual gateway. Drag and drop the snippet from the bottom onto the blank in the graphic to finish the message filter syntax. Not all snippets are used.

Select and Place:



Envelope-sender ==“cisco_123@externally.com”

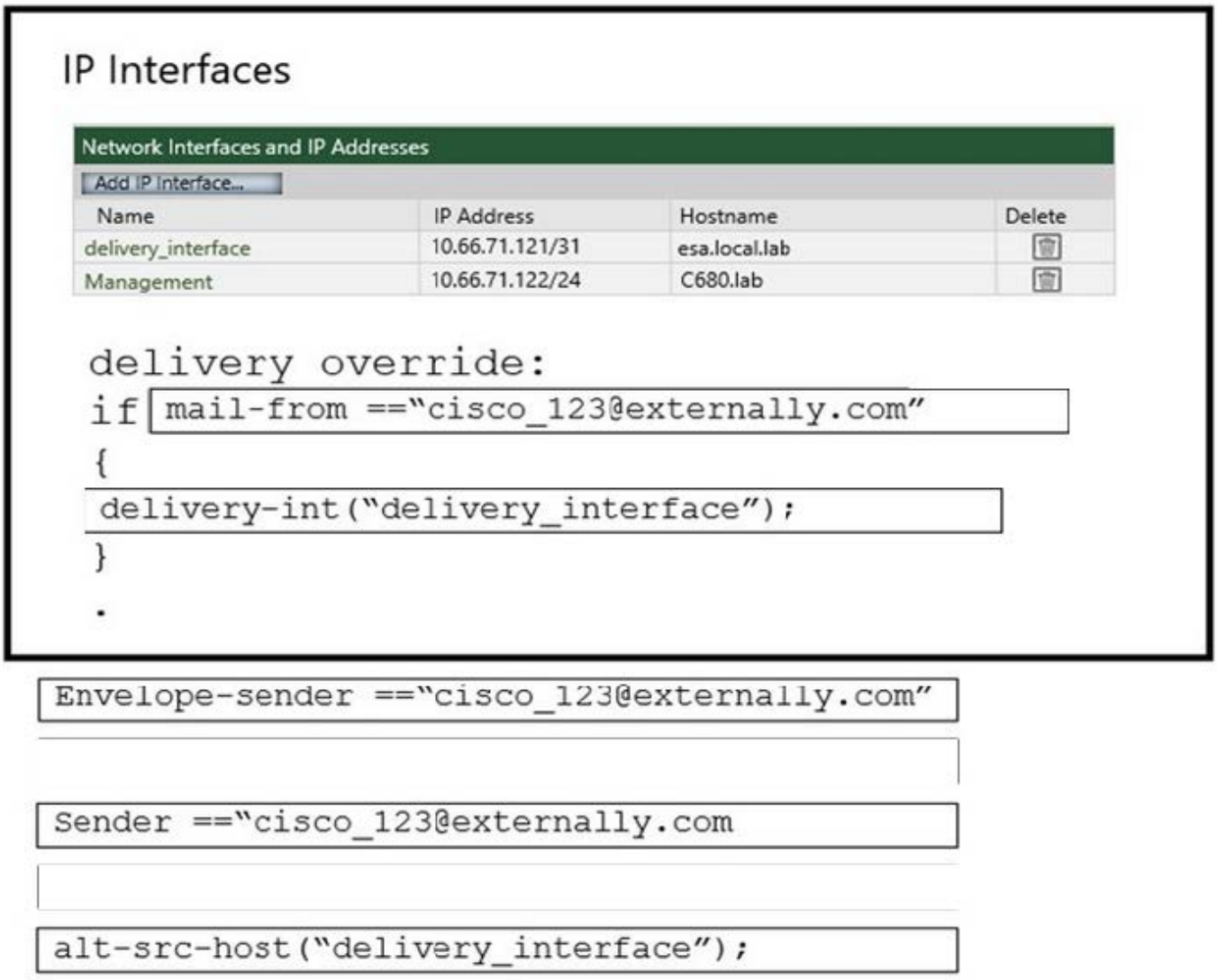
mail-from ==“cisco_123@externally.com”

Sender ==“cisco_123@externally.com

delivery-int(“delivery_interface”);

alt-src-host(“delivery_interface”);

Correct Answer:



QUESTION 8

Which global setting is configured under Cisco ESA Scan Behavior?

A. minimum attachment size to scan

B. attachment scanning timeout

C. actions for unscannable messages due to attachment type

D. minimum depth of attachment recursion to scan

Correct Answer: B

Reference: https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scan-behavior-impact-on-av/td-p/3923243

QUESTION 9

When email authentication is configured on Cisco ESA, which two key types should be selected on the signing profile? (Choose two.)

A. DKIM

B. Public Keys

C. Domain Keys

D. Symmetric Keys

E. Private Keys

Correct Answer: AC

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

QUESTION 10

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

Correct Answer: D

QUESTION 11

The CEO added a sender to a safelist but does not receive an important message expected from the trusted sender. An engineer evaluates message tracking on a Cisco ESA and determines that the message was dropped by the antivirus engine. What is the reason for this behavior?

A. End-user safelists apply to antispam engines only.

B. The sender didn\\'t mark the message as urgent.

C. Administrative access is required to create a safelist.

D. The sender is included in an ISP blocklist.

Correct Answer: A

QUESTION 12

Which feature must be activated on a Cisco ESA to combat backscatter?

A. Graymail Detection

B. Bounce Profile

C. Forged Email Detection

D. Bounce Verification

Correct Answer: D

QUESTION 13

An organization has strict rules for meeting specific criteria to approve certificate authorities. A Cisco ESA administrator within the organization is receiving complaints about failed inbound emails from a domain. The administrator is also seeing TLS certificate errors. What is the reason for this issue?

A. Firewall inspection is preventing transmission of certificate data.

B. The certificate authority is not on the system list.

C. The TLSv1.0 protocol is not supported.

D. The certificate chain is broken.

Correct Answer: D

QUESTION 14

DRAG DROP

Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.

Select and Place:

Associate the filter with a nominated incoming mail policy.	step 1
Configure a filter to take necessary action on SPF/SIDF verification results.	step 2
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	step 3
Test the results of message verification.	step 4
Configure a sendergroup to use the custom mail-flow policy.	step 5

Correct Answer:

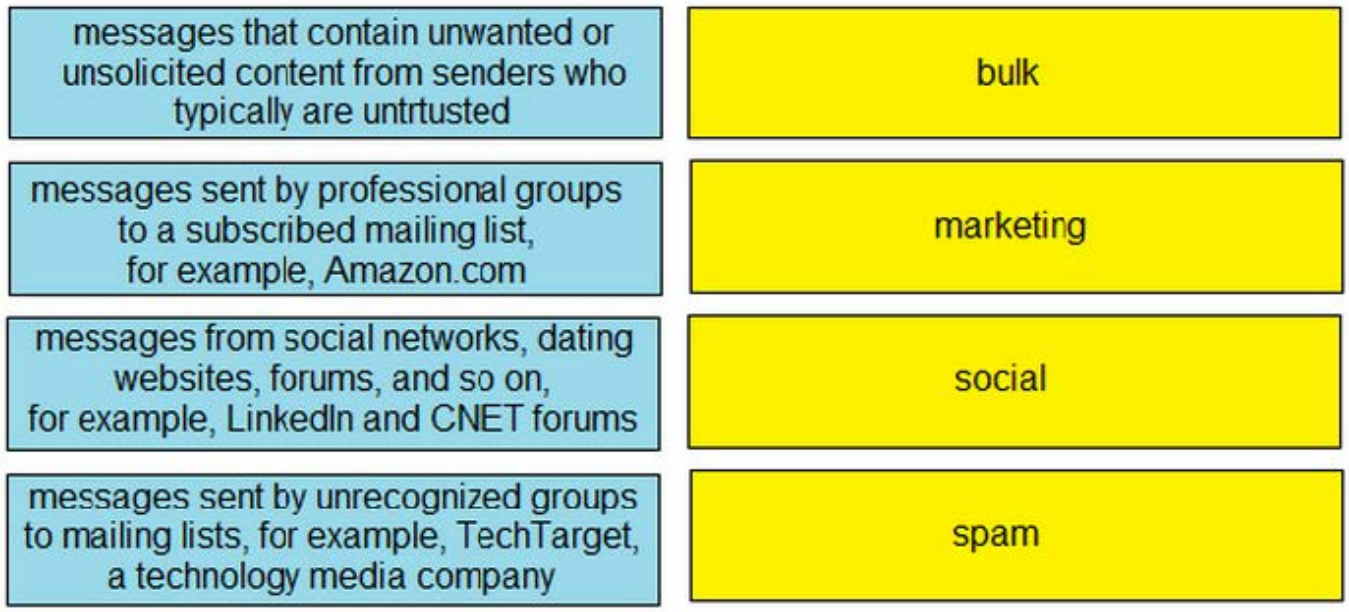
	Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.
	Configure a sendergroup to use the custom mail-flow policy.
	Associate the filter with a nominated incoming mail policy.
	Configure a filter to take necessary action on SPF/SIDF verification results.
	Test the results of message verification.

QUESTION 15

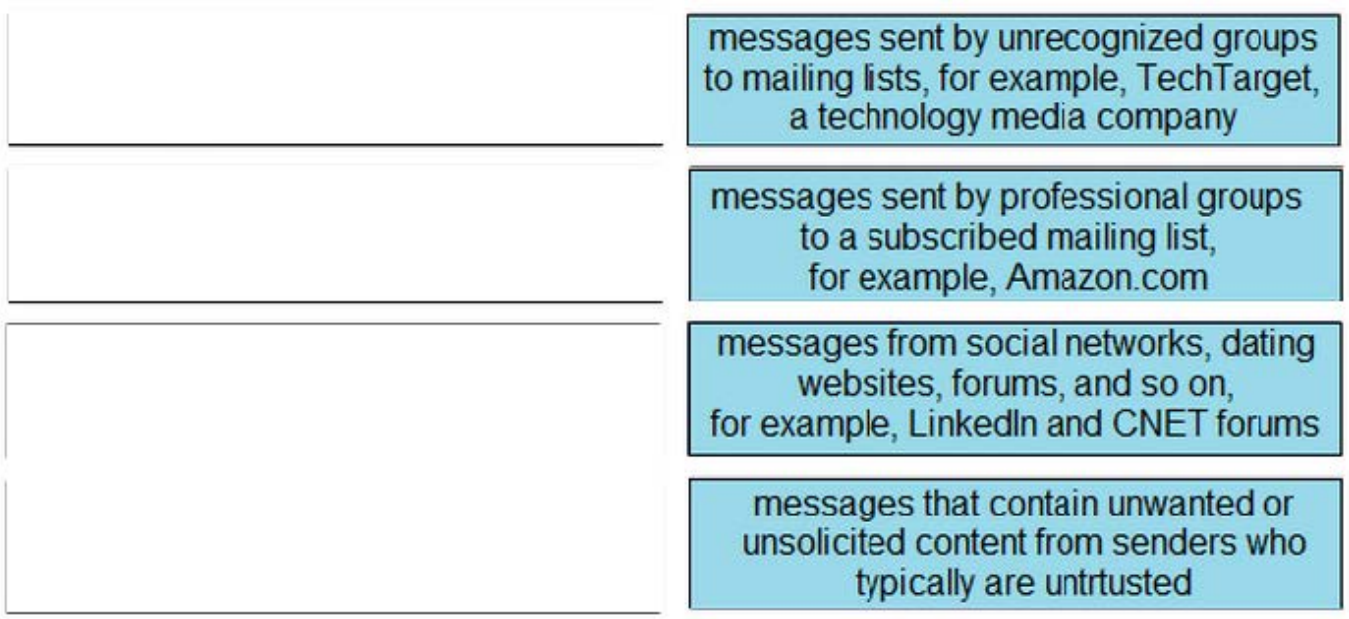
DRAG DROP

Drag and drop the graymail descriptions from the left onto the verdict categories they belong to on the right.

Select and Place:



Correct Answer:



[300-720 PDF Dumps](#) [300-720 Study Guide](#) [300-720 Exam Questions](#)