Free Questions for 300-720 by actualtestdumps

Shared by Ingram on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which component must be added to the content filter to trigger on failed SPF Verification or DKIM Authentication verdicts?

Options:

A- status

B- response

C- parameter

D- condition

Answer:

D

Explanation:

Condition is a component that must be added to the content filter to trigger on failed SPF Verification or DKIM Authentication verdicts.
Condition is a criterion that determines whether a message matches a content filter rule or not, such as message size, sender address,

attachment type, etc.

To add a condition to the content filter that triggers on failed SPF Verification or DKIM Authentication verdicts, the administrator can follow these steps:

Select Mail Policies > Content Filters and click Add Filter.

Enter a name and description for the content filter.

Under Conditions, click Add Condition.

Choose SPF Verification or DKIM Authentication from the drop-down menu.

Choose Fail from the drop-down menu.

Click Submit.

The other options are not valid components to trigger on failed SPF Verification or DKIM Authentication verdicts, because they are not part of content filters.

Question 2

Question Type: **MultipleChoice**

An engineer is configuring an SMTP authentication profile on a Cisco ESA which requires certificate verification.

Which section must be configured to accomplish this goal?

Options:

A- Mail Flow Policies

B- Sending Profiles

C- Outgoing Mail Policies

D- Verification Profiles

Answer:

A

Question 3

Question Type: **MultipleChoice**

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?

Options:

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

B- Use the deli very config 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.

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_12_0_chapter_011001.html

one of the steps to accept mail for additional internal domains on the Cisco ESA is to choose Network > SMTP Routes and enter the new domain and the corresponding destination host IP address1.This can also be done using the smtproutes command in the CLI1. The other commands (deliveryconfig, dsestconf, and altrchost) are not related to this task.

Question 4

Question Type: MultipleChoice

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?

Options:

A- Exception List

B- Connection Behavior

C- Bounce Detection Signing

D- Reverse Connection Verification

Answer:

B

Explanation:

Connection Behavior setting allows you to specify how the Cisco Email Security Appliance (ESA) handles incoming connections from different sender groups. You can choose from four different settings:

Accept: The ESA accepts all connections from the sender group and applies the mail flow policy settings to the messages.

Throttle: The ESA limits the number of concurrent connections and messages per connection from the sender group. This can help reduce the impact of spam or malicious traffic on the ESA's performance.

Reject: The ESA rejects all connections from the sender group and returns a 5xx SMTP error code to the sender. This can help block unwanted or abusive senders from reaching your network.

Test: The ESA accepts connections from the sender group but does not deliver the messages to the recipients. Instead, it logs the messages and marks them as test messages. This can help you test the mail flow policy settings before applying them to real traffic.

To modify the Connection Behavior setting for a sender group, you need to do the following steps:

On the ESA, choose Mail Policies > HAT Overview.

Click Edit Settings for the sender group that you want to modify.

In the Mail Flow Policy Settings section, choose one of the options from the Connection Behavior drop-down list.

Click Submit and commit changes.

Question 5

Question Type: **MultipleChoice**

Refer to the exhibits. What must be done to enforce end user authentication before accessing quarantine?

Options:

A- Enable SPAM notification and use LDAP for authentication.

B- Enable SPAM Quarantine Notification and add the %quarantine_url% variable.

C- Change the end user quarantine access from None authentication to SAAS.

D- Change the end user quarantine access setting from None authentication to Mailbox.

Answer:

D

Explanation:

Changing the end user quarantine access setting from None authentication to Mailbox is the correct way to enforce end user authentication before accessing quarantine. This setting requires the end users to enter their email address and password in order to access their personal quarantine on the Cisco ESA.

The other options are not valid ways to enforce end user authentication before accessing quarantine, because they do not affect the end user quarantine access setting.

Question 6

Question Type: MultipleChoice

A network administrator notices that there are a high number of queries to the LDAP server. The mail logs show an entry "550 Too many invalid recipients | Connection closed by foreign host."

Which feature must be used to address this?

Options:

A- DHAP

B- SBRS

C- LDAP

D- SMTP

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_12_0_chapter_011010.html

DHAP (Directory Harvest Attack Prevention) is a feature that must be used to address this issue. DHAP is a mechanism that allows Cisco ESA to prevent directory harvest attacks, which are attempts by spammers or hackers to obtain valid email addresses from an LDAP server by sending messages with random or guessed recipients and checking for bounce messages.

To enable DHAP on Cisco ESA, the network administrator can follow these steps:

Select Network > Listeners and click Edit Settings for the listener that receives incoming messages.

Under SMTP Authentication Settings, select Enable Directory Harvest Attack Prevention.

Enter a value for Maximum Invalid Recipients per Hour, which is the number of invalid recipients that triggers DHAP.

Enter a value for Block Sender for (hours), which is the duration that Cisco ESA blocks messages from senders who exceed the maximum invalid recipients per hour.

Click Submit.

Question 7

Question Type: MultipleChoice

Refer to the exhibit. What is the correct order of commands to set filter 2 to active?

Options:

A- filters-> edit-> 2-> Active

B- filters-> modify-> All-> Active

C- filters-> detail-> 2-> 1

D- filters-> set-> 2-> 1

Answer:

D

Explanation:

The correct order of commands to set filter 2 to active on the CLI of Cisco ESA is:

filters, which enters the message filter mode.

set, which sets the status of one or more message filters.

2, which specifies the message filter number.

1, which sets the status of message filter 2 to active.

The other options are not valid orders of commands to set filter 2 to active on the CLI of Cisco ESA, because they use incorrect commands or parameters.

Question 8

Question Type: MultipleChoice

Users have been complaining of a higher volume of emails containing profanity. The network administrator will need to leverage dictionaries and create specific conditions to reduce the number of inappropriate emails.

Which two filters should be configured to address this? (Choose two.)

Options:

A- message

B- spam

C- VOF

D- sender group

E- content

Answer:

A, E

Explanation:

Message filter and content filter are two filters that should be configured to address this issue. Message filter and content filter are rules that allow Cisco ESA to perform actions on messages based on predefined or custom conditions, such as headers, envelope, body, attachments, etc.

To reduce the number of inappropriate emails containing profanity, the network administrator can create a dictionary that contains a list of profane words or phrases and use it as a condition in a message filter or content filter that applies an action of "drop", "quarantine", or "modify subject" on the matching messages.

The other options are not valid filters to address this issue, because they do not use dictionaries or conditions based on message content.

Question 9

Question Type: MultipleChoice

Refer to the exhibit. Which configuration on the scan behavior must be updated to allow the attachment to be scanned on the Cisco ESA?

Options:

A- Add an additional mapping for attachment type for zip files.

B- Enable assume match pattern if the email was not scanned for any reason.

C- Increase the maximum recursion depth from 5 to a larger value.

D- Increase the maximum attachment size to scan to a larger value.

Answer:

D

Explanation:

The maximum attachment size to scan is a configuration on the scan behavior that determines the maximum size of an attachment that Cisco ESA will scan for viruses and malware. If an attachment exceeds this size, Cisco ESA will apply the configured action for unscannable messages, such as deliver, drop, or quarantine.

To allow the attachment to be scanned on the Cisco ESA, this configuration must be updated to a larger value than the attachment size, which is 10 MB according to the message header.

The other options are not valid configurations to allow the attachment to be scanned on the Cisco ESA, because they do not affect the maximum attachment size to scan.

Question 10

Question Type: MultipleChoice

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?

Options:

A- file reputation filtering

B- outbreak filtering

C- data loss prevention

D- file analysis

Answer:

C

Explanation:

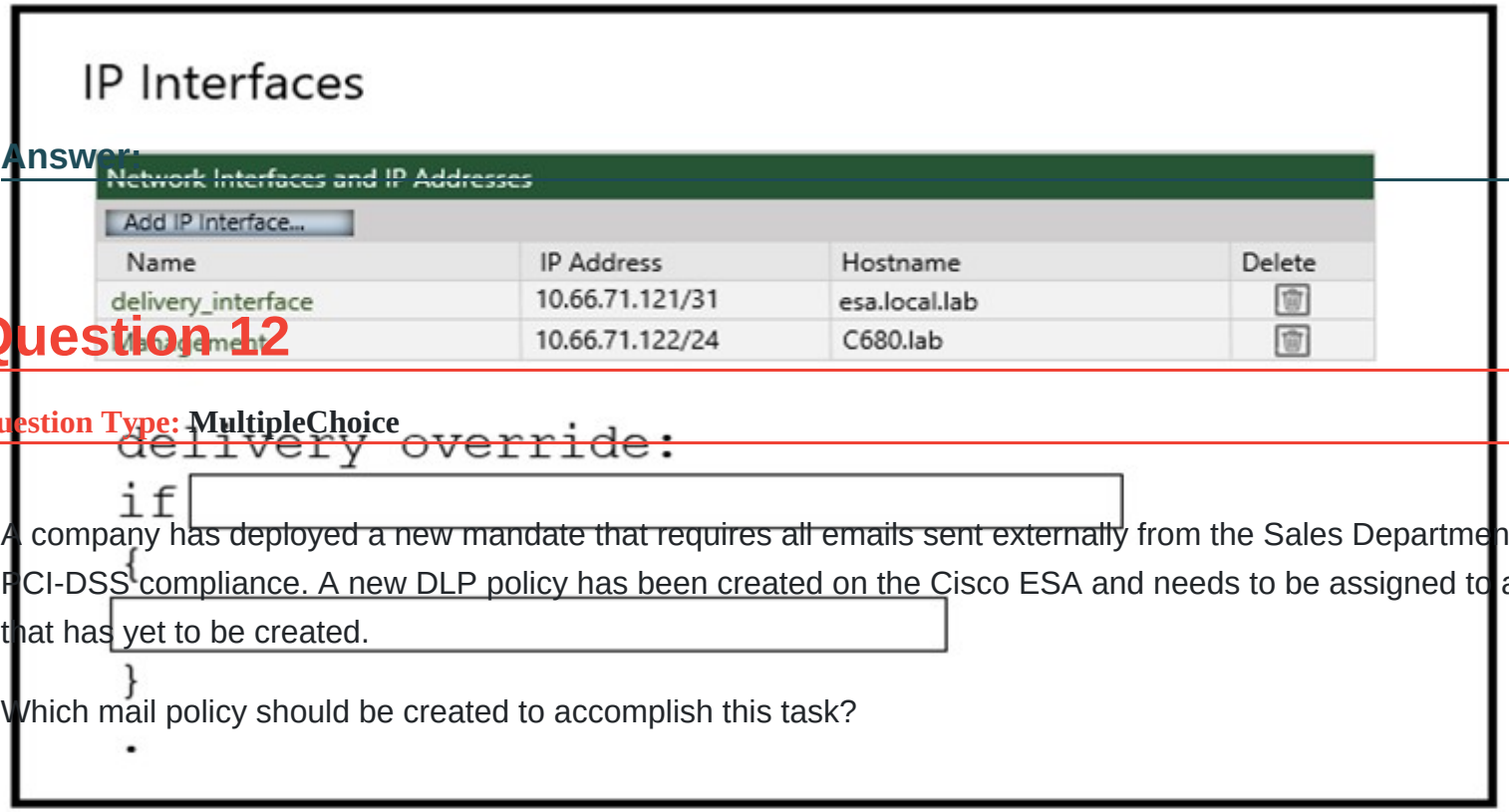
Data Loss Prevention (DLP) is an outgoing mail policy feature that should be configured to catch this content before it leaves the network. DLP allows Cisco ESA to scan outgoing messages for sensitive or confidential data, such as credit card numbers, social security numbers, health records, etc., and apply appropriate actions, such as encrypt, quarantine, notify, etc., to prevent data leakage or loss.

The other options are not valid outgoing mail policy features to catch this content before it leaves the network, because they do not scan for sensitive or confidential data in messages.

Question 11

Question Type: DragDrop

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.



Answer:

Question 12

Question Type: MultipleChoice

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?

Envelope-sender ==“cisco_123@externally.com” n”
mail-from ==“cisco_123@externally.com”
Sender ==“cisco_123@externally.com m
delivery_int(“delivery_interface”); ;
alt-src-host(“delivery_interface”);’);

Options:

A- Outgoing Mail Policy

B- Preliminary Mail Policy

C- Incoming Mail Flow Policy

D- Outgoing Mail Flow Policy

Answer:

A

Explanation:

Outgoing Mail Policy is a mail policy that should be created to accomplish this task. Outgoing Mail Policy is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.

To create an Outgoing Mail Policy named 'Sales' and assign a DLP policy to it, the administrator can follow these steps:

Select Mail Policies > Outgoing Mail Policies and click Add Policy.

Enter 'Sales' as the policy name and click Submit.

Select 'Sales' from the list of policies and click Edit Settings.

Under Data Loss Prevention, select Enable Data Loss Prevention Scanning and choose the DLP policy from the drop-down menu.

Click Submit.

The other options are not valid mail policies to accomplish this task, because they do not apply to outgoing messages or DLP scanning.