Cisco.300-720.vJun-2024.Quan.100q

Number: 300-720
Passing Score: 800
Time Limit: 120
File Version: 11.0

Exam Code: 300-720

Exam Name: Securing Email with Cisco Email Security Appliance (300-720 SESA)

Exam A

QUESTION 1
Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?

A. Set up the interface group with the flag.
B. Issue the altsrchost command.
C. Map the envelope sender address to the host.
D. Apply a filter on the message.

Correct Answer: B
Section:
Explanation:
The altsrchost command enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way. This command allows you to specify an alternate source host for messages that match a message filter. You can use this command to route messages to different virtual gateways based on the message content or attributes.
Reference: Securing Email with Cisco Email Security Appliance (SESA) v3.1, Module 5: Using Message Filters to Enforce Email Policies, Lesson 1: Using Message Filters
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01000.html#con_1133810

QUESTION 2
An administrator is trying to enable centralized PVO but receives the error, "Unable to proceed with
Centralized Policy, Virus and Outbreak Quarantines configuration as esa1 in Cluster has content filters / DLP actions available at a level different from the cluster level."
What is the cause of this error?

A. Content filters are configured at the machine-level on esa1.
B. DLP is configured at the cluster-level on esa2.
C. DLP is configured at the domain-level on esa1.
D. DLP is not configured on host1.

Correct Answer: D
Section:
Explanation:
The PVO cannot be enabled and shows this type of error message.
Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines configuration as host1 and host2 in Cluster have content filters / DLP actions available at a level different from the cluster Level.
The error message can indicate that one of the hosts does not have a DLP feature key applied and DLP is disabled. The solution is to add the missing feature key and apply DLP settings identical as on the host that has the feature key applied. This feature key inconsistency might have the same effect with Outbreak Filters, Sophos Antivirus, and other feature keys.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technoteesa-00.html
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote- esa-00.html

QUESTION 3
Which feature must be configured before an administrator can use the outbreak filter for nonviral threats?

A. quarantine threat level
B. antispam
C. data loss prevention
D. antivirus

Correct Answer: B
Section:
Explanation:
The feature that must be configured before an administrator can use the outbreak filter for nonviral threats is antispam. The outbreak filter relies on the antispam engine to detect and block nonviral threats, such as phishing, malware, or spam campaigns. You need to enable antispam scanning and configure the antispam settings before you can use the outbreak filter.
Reference: Securing Email with Cisco Email Security Appliance (SESA) v3.1, Module 8: Using Anti-Virus and Outbreak Filters, Lesson 2: Configuring Outbreak Filters
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_chapter_01110.html

QUESTION 4
Which type of attack is prevented by configuring file reputation filtering and file analysis features?

A. denial of service
B. zero-day
C. backscatter
D. phishing

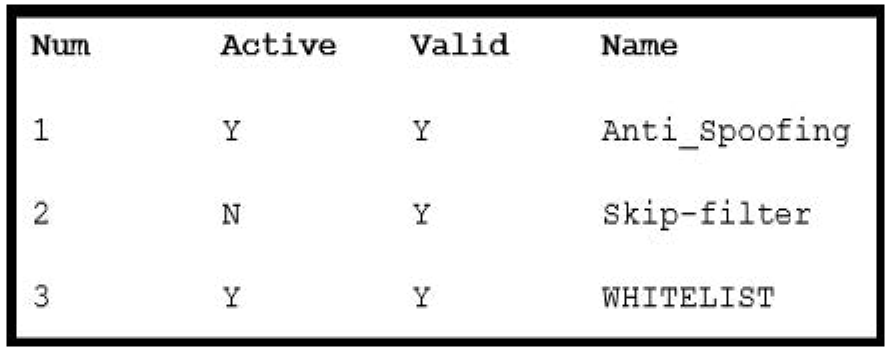
Correct Answer: B
Section:
Explanation:
The type of attack that is prevented by configuring file reputation filtering and file analysis features is zero-day. Zero-day attacks are those that exploit unknown vulnerabilities in software or systems before they are patched or fixed. File reputation filtering and file analysis features help to protect against zero-day attacks by checking the reputation of files attached to email messages and sending them to a cloud-based service for dynamic analysis.
Reference: Securing Email with Cisco Email Security Appliance (SESA) v3.1, Module 9: Using Advanced Malware Protection, Lesson 1: Configuring File Reputation Filtering and File Analysis
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_chapter_010000.html#con_1809885

QUESTION 5
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.)

A. message
B. spam
C. VOF
D. sender group
E. content

Correct Answer: A, E
Section:
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.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-3 and page 8-7.

QUESTION 6



Num	Active	Valid	Name
1	Y	Y	Anti_Spoofing
2	N	Y	Skip-filter
3	Y	Y	WHITELIST

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

A. filters-> edit-> 2-> Active
B. filters-> modify-> All-> Active
C. filters-> detail-> 2-> 1
D. filters-> set-> 2-> 1

Correct Answer: D
Section:
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.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page A-6 and page A-7.

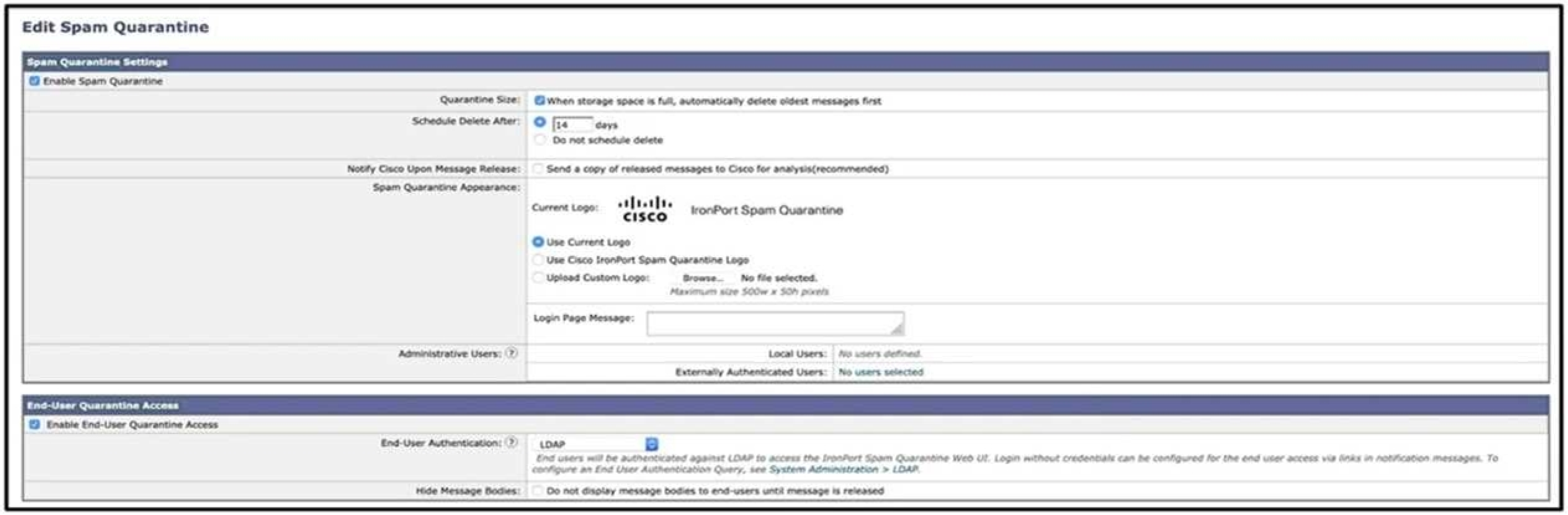
QUESTION 7

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?

A. DHAP
B. SBRS
C. LDAP
D. SMTP

Correct Answer: A
Section:
Explanation:
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_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 8



Edit Spam Quarantine

Spam Quarantine Settings

☑ Enable Spam Quarantine

Quarantine Size: ☑ When storage space is full, automatically delete oldest messages first

Schedule Delete After: ● 14 days
○ Do not schedule delete

Notify Cisco Upon Message Release: □ Send a copy of released messages to Cisco for analysis(recommended)

Spam Quarantine Appearance:

Current Logo: CISCO IronPort Spam Quarantine

● Use Current Logo

○ Use Cisco IronPort Spam Quarantine Logo

○ Upload Custom Logo: Browse... No file selected.

Maximum size 500w x 50h pixels

Login Page Message:

Administrative Users: ?

Local Users: *No users defined.*

Externally Authenticated Users: No users selected

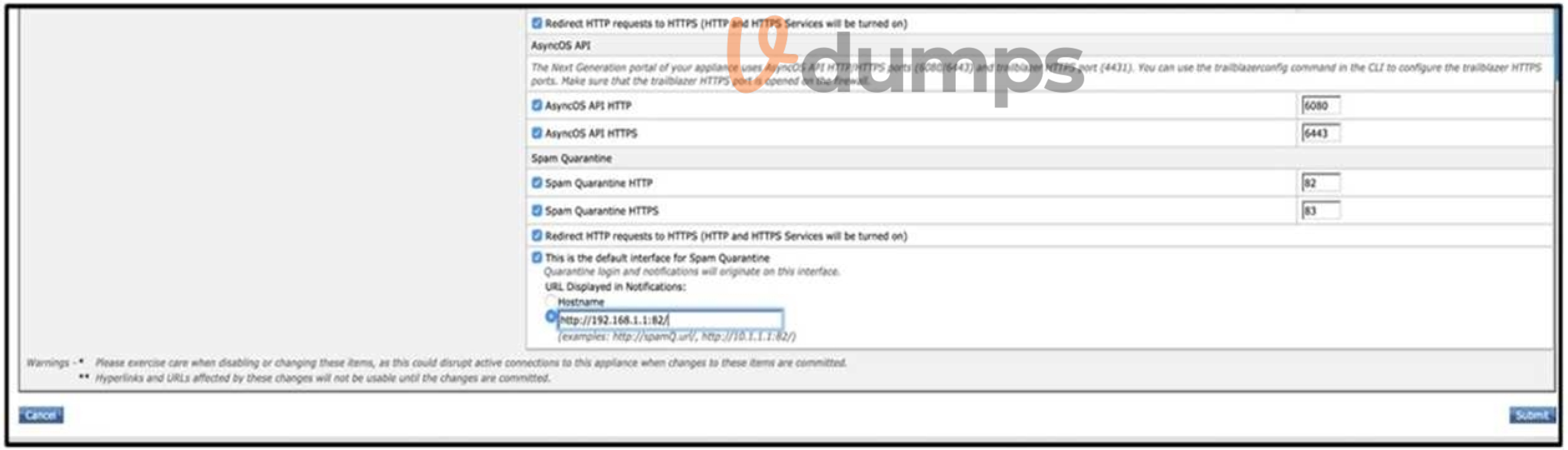
End-User Quarantine Access

☑ Enable End-User Quarantine Access

End-User Authentication: ? LDAP

End users will be authenticated against LDAP to access the IronPort Spam Quarantine Web UI. Login without credentials can be configured for the end user access via links in notification messages. To configure an End User Authentication Query, see System Administration > LDAP.

Hide Message Bodies: □ Do not display message bodies to end-users until message is released



☑ Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)

AsyncOS API

The Next Generation portal of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazerconfig command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.

☑ AsyncOS API HTTP 6080

☑ AsyncOS API HTTPS 6443

Spam Quarantine

☑ Spam Quarantine HTTP 82

☑ Spam Quarantine HTTPS 83

☑ Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)

☑ This is the default interface for Spam Quarantine

Quarantine login and notifications will originate on this interface.

URL Displayed in Notifications:

○ Hostname

● http://192.168.1.1:82/

(examples: http://spamQ.url/, http://10.1.1.1:82/)

*Warnings - * Please exercise care when disabling or changing these items, as this could disrupt active connections to this appliance when changes to these items are committed.*

*** Hyperlinks and URLs affected by these changes will not be usable until the changes are committed.*

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

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.

Correct Answer: D

Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure-esa-00.html#anc7
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.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-2 and page 10-3.

QUESTION 9
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
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html
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 10
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 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.

Correct Answer: A
Section:
Explanation:
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_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 11
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?

A. Mail Flow Policies
B. Sending Profiles
C. Outgoing Mail Policies
D. Verification Profiles

Correct Answer: A
Section:

QUESTION 12
Which SMTP extension does Cisco ESA support for email security?

A. ETRN
B. UTF8SMTP
C. PIPELINING
D. STARTTLS

Correct Answer: D
Section:
Explanation:
STARTTLS is an SMTP extension that allows email servers to negotiate a secure connection using TLS or SSL encryption. Cisco ESA supports STARTTLS for both inbound and outbound email delivery.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 5-2.
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 13
Which feature utilizes sensor information obtained from Talos intelligence to filter email servers connecting into the Cisco ESA?

A. SenderBase Reputation Filtering
B. Connection Reputation Filtering
C. Talos Reputation Filtering
D. SpamCop Reputation Filtering

Correct Answer: A
Section:
Explanation:
SenderBase Reputation Filtering is a feature that allows Cisco ESA to reject or throttle connections from email servers based on their reputation score, which is calculated by Talos using sensor information from various sources.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-2.

QUESTION 14
When the Spam Quarantine is configured on the Cisco ESA, what validates end-users via LDAP during login to the End-User Quarantine?

A. Enabling the End-User Safelist/Blocklist feature
B. Spam Quarantine External Authentication Query

C. Spam Quarantine End-User Authentication Query
D. Spam Quarantine Alias Consolidation Query

Correct Answer: C
Section:
Explanation:
Spam Quarantine End-User Authentication Query is a query that Cisco ESA performs against an LDAP server to validate the end-user credentials during login to the End-User Quarantine.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-9.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure- esa-00.html

QUESTION 15
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
Section:
Explanation:
External spam quarantine is a feature that allows Cisco SMA to store and manage spam messages quarantined by multiple Cisco ESAs in one central location, providing a unified view and administration of the spam quarantine data.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-3.
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 16
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: B, E
Section:
Explanation:
With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography. Configuring DomainKeys and DKIM Signing A signing key is the private key stored on the appliance.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_010101.html?bookSearch=true

QUESTION 17
What are two phases of the Cisco ESA email pipeline? (Choose two.)

A. reject
B. workqueue
C. action

D. delivery
E. quarantine

Correct Answer: B, D
Section:
Explanation:
With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography. Configuring DomainKeys and DKIM Signing A signing key is the private key stored on the appliance.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_010101.html?bookSearch=true
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-1/user_guide/b_ESA_Admin_Guide_12_1/b_ESA_Admin_Guide_12_1_chapter_011.pdf (p.1)

QUESTION 18
Which two action types are performed by Cisco ESA message filters? (Choose two.)

A. non-final actions
B. filter actions
C. discard actions
D. final actions
E. quarantine actions

Correct Answer: A, D
Section:
Explanation:
Non-final actions are actions that do not terminate the message filter evaluation, such as adding headers, setting variables, logging, etc. Final actions are actions that end the message filter evaluation and determine the fate of the message, such as accept, drop, bounce, quarantine, etc.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 3-4.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01000.html

QUESTION 19
Which setting affects the aggressiveness of spam detection?

A. protection level
B. spam threshold
C. spam timeout
D. maximum depth of recursion scan

Correct Answer: B
Section:
Explanation:
Spam threshold is a setting that determines the minimum score that a message must have to be classified as spam by Cisco ESA. The lower the threshold, the more aggressive the spam detection is.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-5.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118220-technote- esa-00.html

QUESTION 20
What is the order of virus scanning when multilayer antivirus scanning is configured?

A. The default engine scans for viruses first and the McAfee engine scans for viruses second.
B. The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.
C. The McAfee engine scans for viruses first and the default engine scans for viruses second.

D. The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.

Correct Answer: D
Section:
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_chapter_01011.html
According to the User Guide for AsyncOS 12.0 for Cisco Email Security Appliances2, the order of virus scanning when multilayer antivirus scanning is configured is as follows:
The McAfee engine scans the message first. If the McAfee engine detects a virus, the message is dropped or repaired, depending on the configuration. If the McAfee engine does not detect a virus, the message is passed to the next layer of scanning.
The Sophos engine scans the message second. If the Sophos engine detects a virus, the message is dropped or repaired, depending on the configuration. If the Sophos engine does not detect a virus, the message is delivered to the recipient.

QUESTION 21
Which antispam feature is utilized to give end users control to allow emails that are spam to be delivered to their inbox, overriding any spam verdict and action on the Cisco ESA?

A. end user allow list
B. end user spam quarantine access
C. end user passthrough list
D. end user safelist

Correct Answer: D
Section:
Explanation:
End user safelist is a feature that allows end users to specify email addresses or domains that they want to receive messages from, regardless of the spam verdict or action assigned by Cisco ESA.
Messages from senders on the end user safelist are delivered to the end user's inbox without any spam filtering.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-13.

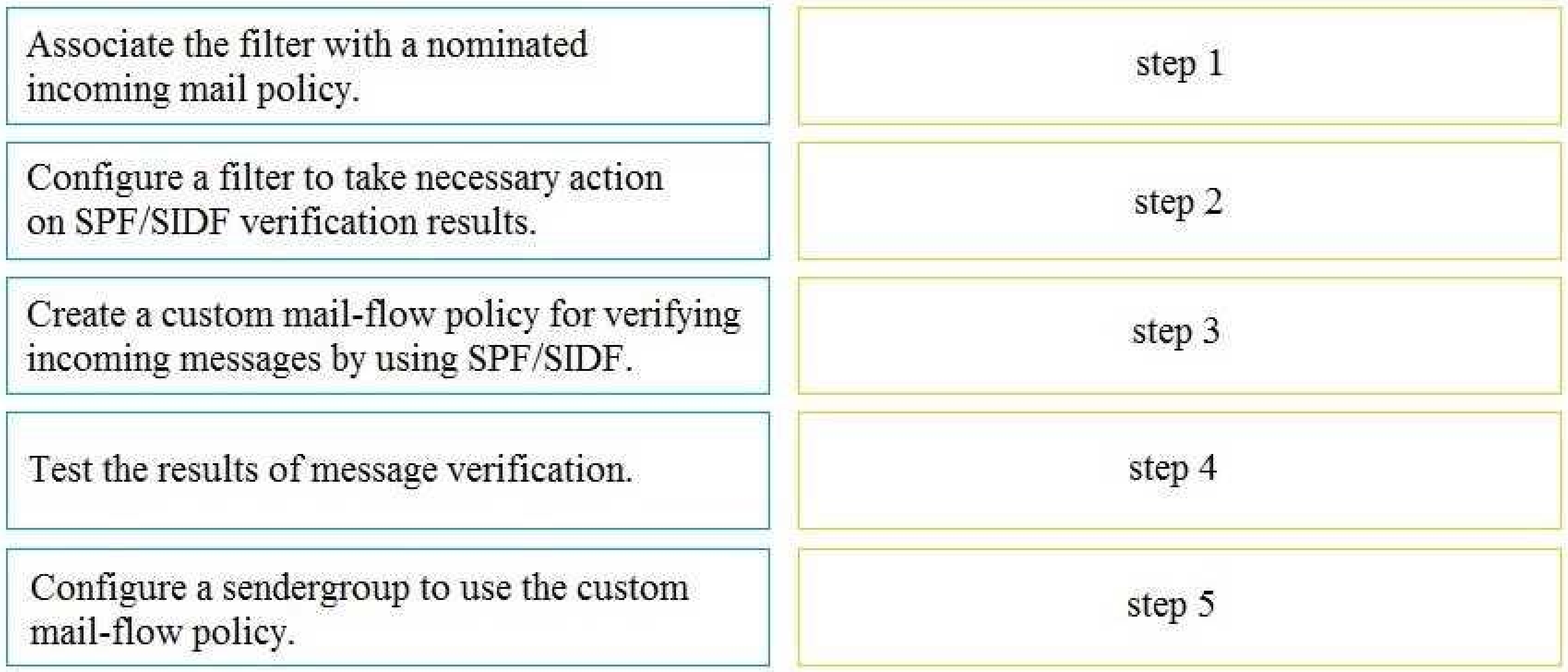
QUESTION 22
What are two prerequisites for implementing undesirable URL protection in Cisco ESA? (Choose two.)

A. Enable outbreak filters.
B. Enable email relay.
C. Enable antispam scanning.
D. Enable port bouncing.
E. Enable antivirus scanning.

Correct Answer: A, C
Section:
Explanation:
Undesirable URL protection is a feature that allows Cisco ESA to detect and block messages that contain URLs that lead to malicious or unwanted websites, such as phishing, malware, or adult content sites. To enable this feature, outbreak filters and antispam scanning must be enabled on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-17.
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_chapter_01111.html

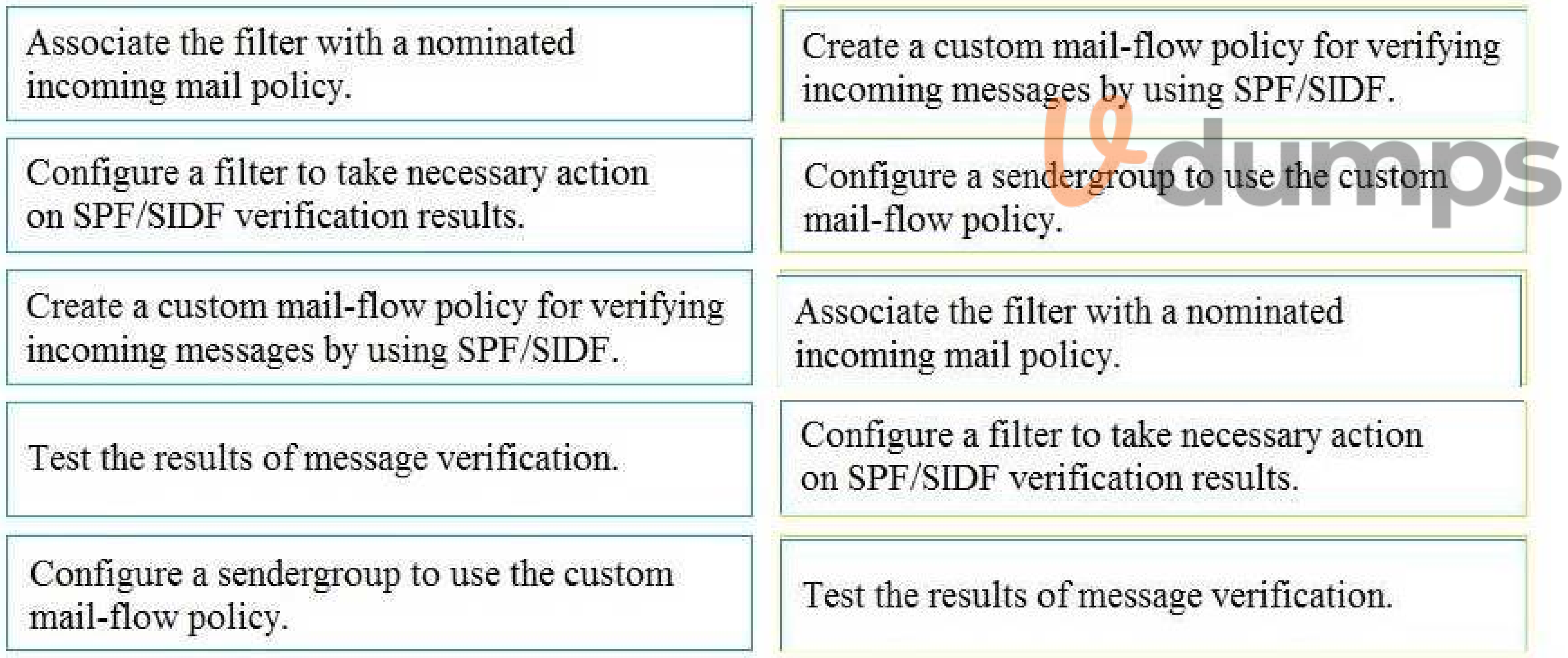
QUESTION 23
DRAG DROP
Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.

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:



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

Section:
Explanation:

QUESTION 24
Which suboption must be selected when LDAP is configured for Spam Quarantine End-User Authentication?

A. Designate as the active query
B. Update Frequency
C. Server Priority

D. Entity ID

Correct Answer: A
Section:
Explanation:
According to the User Guide1, the steps to configure End-User Access to the Spam Quarantine via LDAP are as follows:
On the ESA, choose System Administration > LDAP > LDAP Server Profile page.
Click Add LDAP Server Profile.
Enter a name for the profile and click Submit.
Click Add Query.
Enter a name for the query and click Submit.
Configure the query settings, such as server address, port number, base DN, scope, filter, and attributes.
Check the Spam Quarantine End-User Authentication Query check box. This is the suboption that enables LDAP authentication for end users who access the spam quarantine.
Check the Designate as the active query check box. This is the suboption that specifies which query to use for end-user authentication. Only one query can be active at a time.
Click Submit and commit changes.
On the ESA, choose Monitor > Spam Quarantine > End-User Quarantine Access.
Check the Enable End-User Quarantine Access check box.
Choose LDAP from the End-User Authentication drop-down list.
Select the LDAP profile and query that you created earlier from the drop-down lists.
Click Submit and commit changes.
Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-5/user_guide/ b_SMA_Admin_Guide_11_5/b_SMA_Admin_Guide_11_5_chapter_01010.html

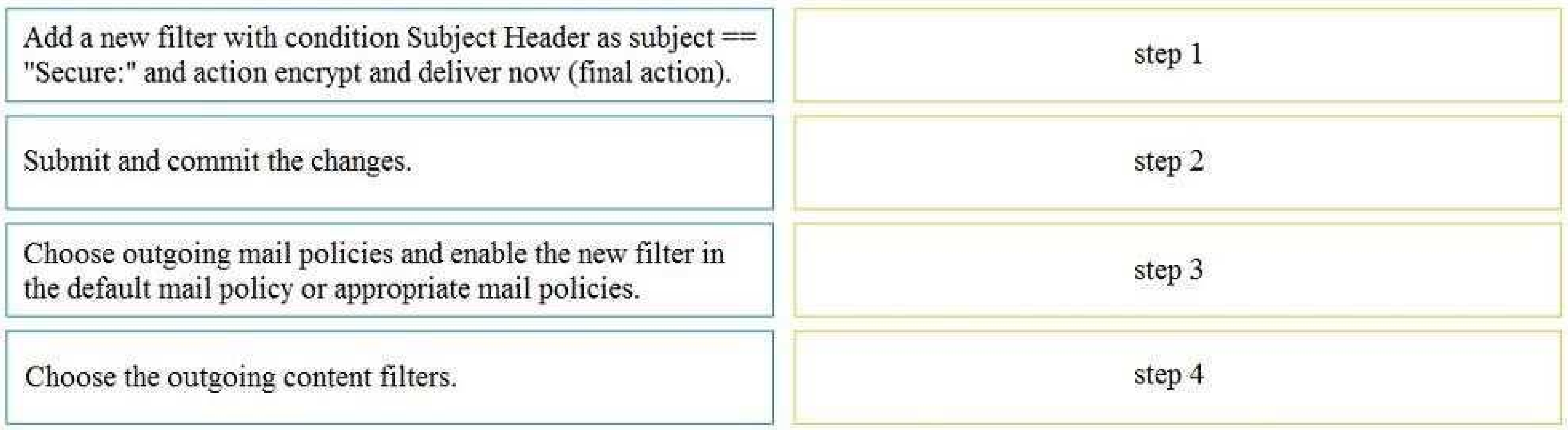
QUESTION 25
Which action must be taken before a custom quarantine that is being used can be deleted?

A. Delete the quarantine that is assigned to a filter.
B. Delete the quarantine that is not assigned to a filter.
C. Delete only the unused quarantine.
D. Remove the quarantine from the message action of a filter.

Correct Answer: D
Section:
Explanation:
Before a custom quarantine that is being used can be deleted, it must be removed from the message action of any filter that is using it on Cisco ESA. Otherwise, an error message will appear stating that the quarantine cannot be deleted because it is in use.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-5.
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_011111.html

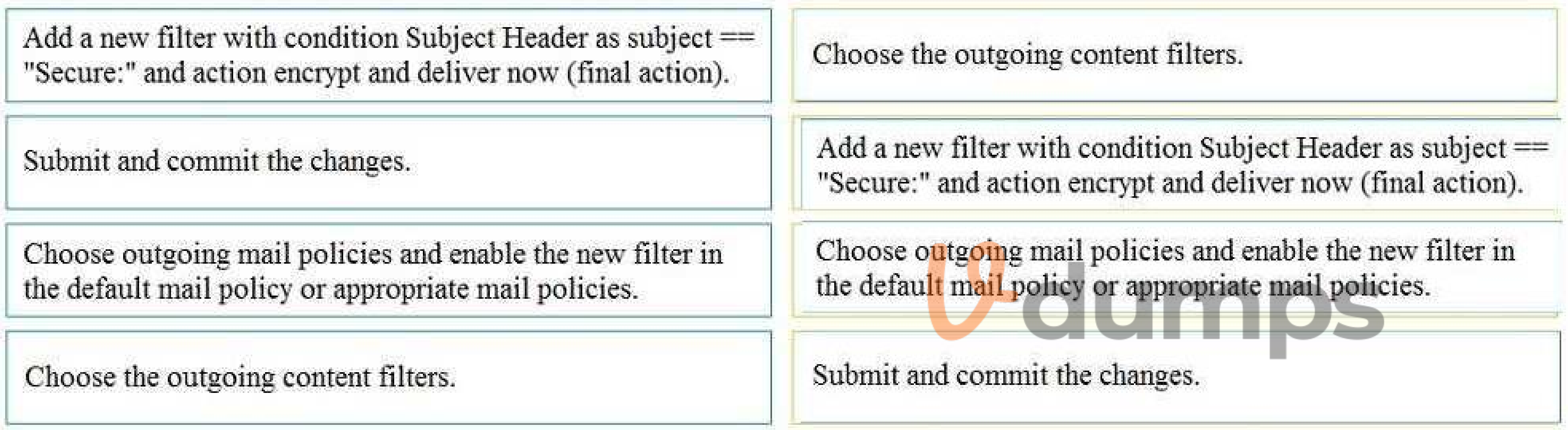
QUESTION 26
DRAG DROP
An Encryption Profile has been set up on the Cisco ESA.
Drag and drop the steps from the left for creating an outgoing content filter to encrypt emails that contains the subject "Secure:" into the correct order on the right.

Select and Place:



Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).	step 1
Submit and commit the changes.	step 2
Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.	step 3
Choose the outgoing content filters.	step 4

Correct Answer:



Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).	Choose the outgoing content filters.
Submit and commit the changes.	Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).
Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.	Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.
Choose the outgoing content filters.	Submit and commit the changes.

Section:
Explanation:
Reference:
https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/tdp/2441383

QUESTION 27
What is the maximum message size that can be configured for encryption on the Cisco ESA?

A. 20 MB
B. 25 MB
C. 15 MB
D. 30 MB

Correct Answer: B
Section:
Explanation:
The maximum message size that can be configured for encryption on the Cisco ESA is 25 MB. This is the default value for the Maximum Message Size for Encryption setting in the Encryption Profile. Messages that exceed this size will not be encrypted and will be delivered as normal.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 12-6.

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117972-technote- esa-00.html

QUESTION 28
An analyst creates a new content dictionary to use with Forged Email Detection.
Which entry will be added into the dictionary?

A. mycompany.com
B. Alpha Beta
C. ^Alpha\ Beta$
D. Alpha.Beta@mycompany.com

Correct Answer: B
Section:
Explanation:
A content dictionary is a list of words or phrases that can be used to match against message content in Cisco ESA. For Forged Email Detection, a content dictionary can be used to specify the display names of internal senders that should not appear in the From header of external messages. The display name is usually the name of the sender as it appears in the email client, such as Alpha Beta. Therefore, the entry that will be added into the dictionary for this purpose is Alpha Beta.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-8.
Reference: https://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/whitepaper_C11-737596.html

QUESTION 29
Which process is skipped when an email is received from safedomain.com, which is on the safelist?

A. message filter
B. antivirus scanning
C. outbreak filter
D. antispam scanning

Correct Answer: D
Section:
Explanation:
The safelist is a list of email addresses or domains that are considered legitimate and trustworthy by Cisco ESA. When an email is received from a sender on the safelist, Cisco ESA skips antispam scanning for that message and delivers it to the recipient without any spam filtering.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-13.

QUESTION 30
Which two query types are available when an LDAP profile is configured? (Choose two.)

A. proxy consolidation
B. user
C. recursive
D. group
E. routing

Correct Answer: B, E
Section:
Explanation:
User and routing are two query types that are available when an LDAP profile is configured on Cisco ESA. User queries are used to validate end-user credentials, such as for Spam Quarantine End-User Authentication or SMTP

Authentication. Routing queries are used to determine the destination mail server for a recipient, such as for Mail Flow Policies or Delivery Methods.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-7.

QUESTION 31
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
Section:
Explanation:
SMTP AUTH is a valid fallback action when a client certificate is unavailable during SMTP authentication on Cisco ESA. SMTP AUTH is a method of authenticating SMTP clients using username and password credentials, which can be verified by an LDAP server or a local database on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 5-10.
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 32
Email encryption is configured on a Cisco ESA that uses CRES.
Which action is taken on a message when CRES is unavailable?

A. It is requeued.
B. It is sent in clear text.
C. It is dropped and an error message is sent to the sender.
D. It is encrypted by a Cisco encryption appliance.

Correct Answer: A
Section:
Explanation:
When CRES (Cisco Registered Envelope Service) is unavailable, Cisco ESA will requeue the message and attempt to resend it later, until the maximum number of retries or the maximum age of the message is reached. The message will not be sent in clear text, dropped, or encrypted by another appliance.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 12-8.

QUESTION 33
Which two features of Cisco Email Security are added to a Sender Group to protect an organization against email threats? (Choose two.)

A. NetFlow
B. geolocation-based filtering
C. heuristic-based filtering
D. senderbase reputation filtering
E. content disarm and reconstruction

Correct Answer: B, D
Section:
Explanation:
Geolocation-based filtering and senderbase reputation filtering are two features of Cisco Email Security that can be added to a Sender Group to protect an organization against email threats. Geolocation-based filtering allows

Cisco ESA to accept or reject connections from email servers based on their geographic location, such as country or continent. Senderbase reputation filtering allows Cisco ESA to reject or throttle connections from email servers based on their reputation score, which is calculated by Talos using sensor information from various sources.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 5-4 and page 6-2.

QUESTION 34
Which two steps configure Forged Email Detection? (Choose two.)

A. Configure a content dictionary with executive email addresses.
B. Configure a filter to use the Forged Email Detection rule and dictionary.
C. Configure a filter to check the Header From value against the Forged Email Detection dictionary.
D. Enable Forged Email Detection on the Security Services page.
E. Configure a content dictionary with friendly names.

Correct Answer: B, E
Section:
Explanation:
Forged Email Detection is a feature that allows Cisco ESA to detect and block messages that spoof the display names of internal senders in the From header, such as executives or managers, to trick recipients into opening malicious or fraudulent emails. To configure this feature, two steps are required:
Configure a content dictionary with friendly names of internal senders that should not appear in the From header of external messages, such as Alpha Beta or John Smith.
Configure a filter to use the Forged Email Detection rule and dictionary, which will compare the display name in the From header of incoming messages with the entries in the content dictionary, and apply the configured action if a match is found.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-8.

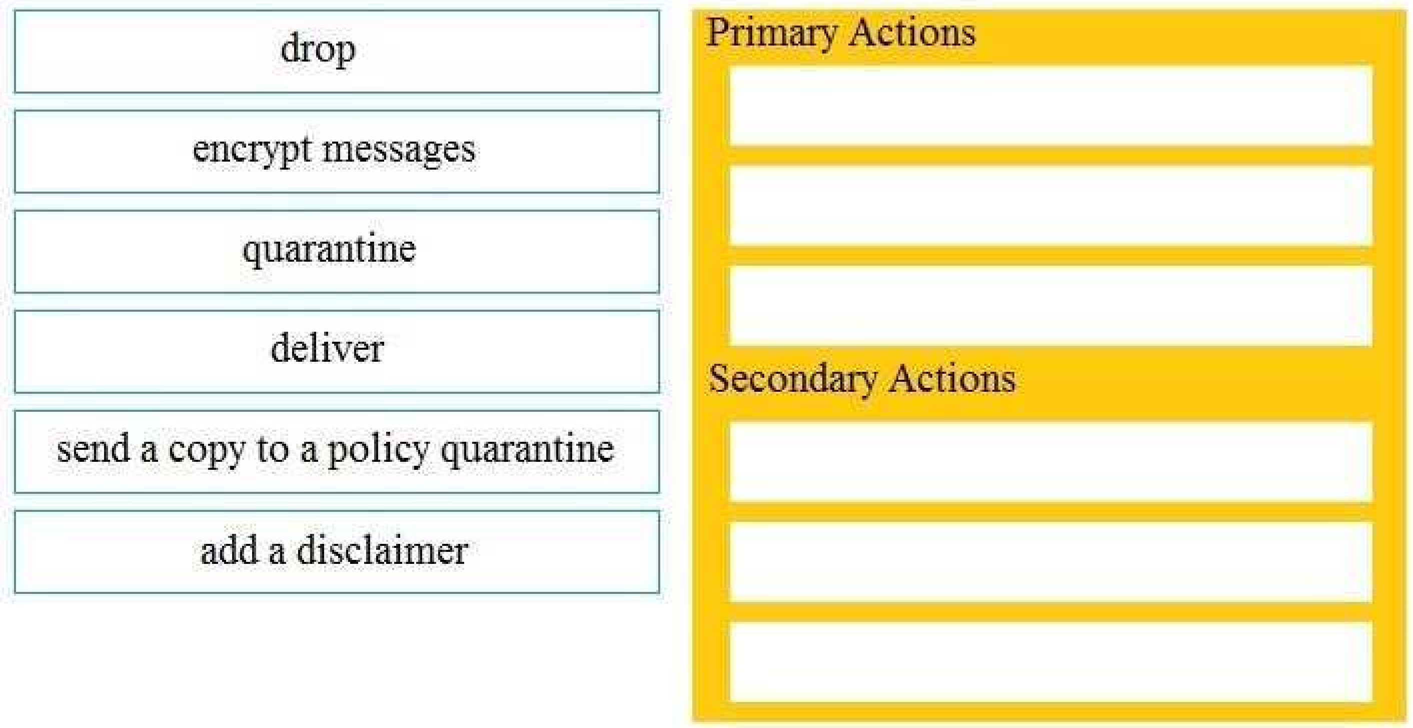
QUESTION 35
What is the default behavior of any listener for TLS communication?

A. preferred-verify
B. off
C. preferred
D. required

Correct Answer: B
Section:
Explanation:
The default behavior of any listener for TLS communication is B. off. This means that TLS is not allowed for incoming connections to the listener and connections to the listener do not require encrypted Simple Mail Transfer Protocol (SMTP) conversations. This is stated in the web search result 1. To enable TLS for a listener, you need to configure the Use TLS option in the mail flow policy settings for the listener on the Mail Policies > HAT Overview page1. You can choose from three different settings for TLS: No, Preferred, or Required1.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118954-config-esa- 00.html

QUESTION 36
DRAG DROP
Drag and drop the Cisco ESA reactions to a possible DLP from the left onto the correct action types on the right.

Select and Place:



drop

encrypt messages

quarantine

deliver

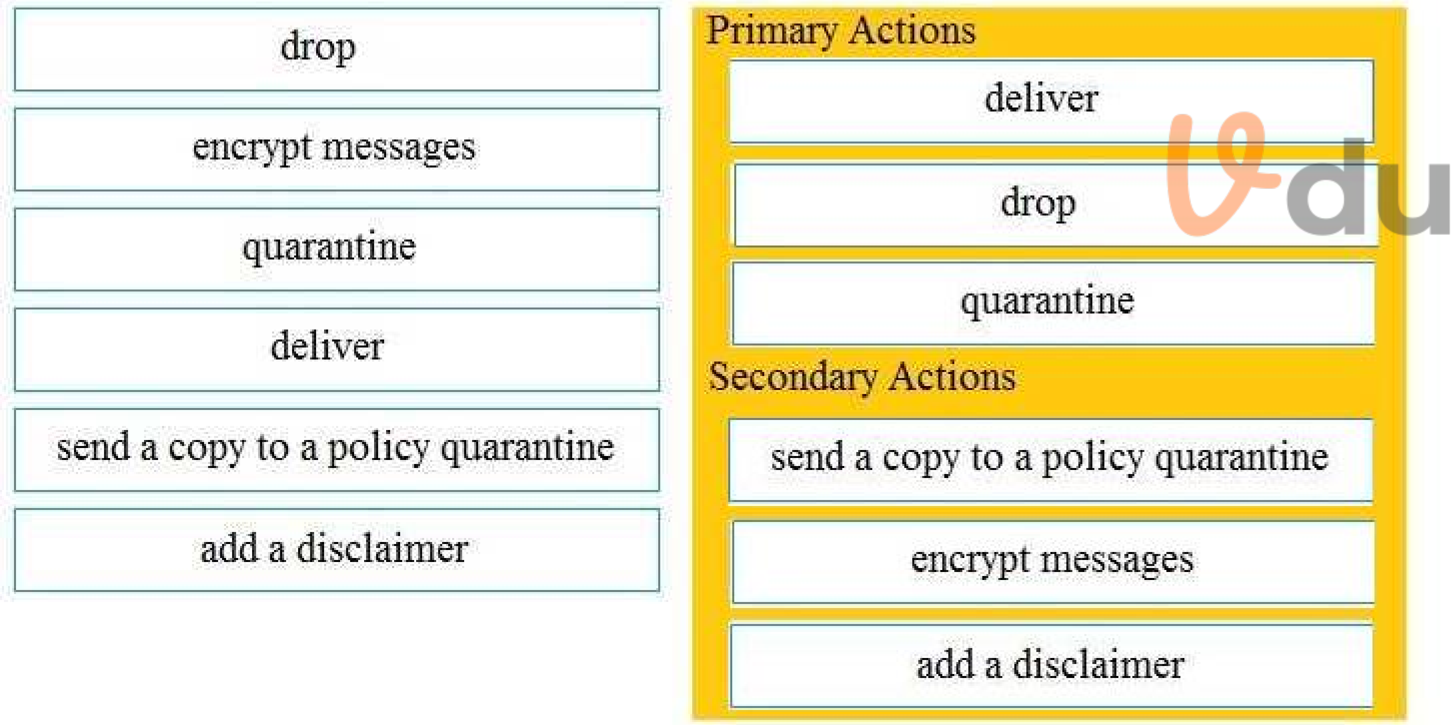
send a copy to a policy quarantine

add a disclaimer

Primary Actions

Secondary Actions

Correct Answer:



drop

encrypt messages

quarantine

deliver

send a copy to a policy quarantine

add a disclaimer

Primary Actions

deliver

drop

quarantine

Secondary Actions

send a copy to a policy quarantine

encrypt messages

add a disclaimer

Section:

Explanation:

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_chapter_010001.html (message actions)

QUESTION 37

Which two actions are configured on the Cisco ESA to query LDAP servers? (Choose two.)

A. accept

B. relay

C. delay
D. route
E. reject

Correct Answer: A, D
Section:
Explanation:
If you store user information within LDAP directories in your network infrastructure you can configure the appliance to query your LDAP servers to accept, route, and authenticate messages.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_011010.html
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_011010.html

QUESTION 38
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: A, D
Section:
Explanation:
Message filters can only be applied to the ESA via command line. So, you will need command line access to the ESA.
Log into the ESA via command line.
Run the following highlighted commands to apply the message filter to the ESA:

```
ironport.example.com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script. Enter '.' on its own line to end.
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
quarantine("large_spam");
log-entry("*****This is a large message with no attachments*****");
}.
1 filters added.
```

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

QUESTION 39
What occurs when configuring separate incoming mail policies?

A. message splintering
B. message exceptions
C. message detachment
D. message aggregation

Correct Answer: A
Section:
Explanation:
Message splintering is a process that occurs when configuring separate incoming mail policies on Cisco ESA. Message splintering means that Cisco ESA will split a single incoming message into multiple copies, each with a different recipient and policy, and apply different security services and actions to each copy.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 4-2.

QUESTION 40
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
Section:
Explanation:
When DKIM (DomainKeys Identified Mail) signing is configured on Cisco ESA, the DNS record that must be updated to load the DKIM public signing key is the TXT record. The TXT record is used to store arbitrary text information in the DNS, such as the DKIM public key, which can be retrieved by the recipients to verify the DKIM signature in the message header.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 11-3.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa- configure-dkim-signing.html

QUESTION 41
What is a valid content filter action?

A. decrypt on delivery
B. quarantine
C. skip antispam
D. archive

Correct Answer: B
Section:
Explanation:
A content filter action is an operation that Cisco ESA performs on a message if it matches the conditions of a content filter rule, such as headers, envelope, body, attachments, etc.
Quarantine is a valid content filter action that allows Cisco ESA to store the message in a quarantine area for further review or release by an administrator or an end user.
The other options are not valid content filter actions on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-3 and page 8-7.
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_chapter_01010.html#con_1158022

QUESTION 42
When virtual gateways are configured, which two distinct attributes are allocated to each virtual gateway address? (Choose two.)

A. domain
B. IP address
C. DNS server address
D. DHCP server address
E. external spam quarantine

Correct Answer: A, B
Section:
Explanation:
Virtual gateways are a feature that allows Cisco ESA to host multiple email domains on a single physical interface, using different IP addresses and hostnames for each domain.
When virtual gateways are configured, two distinct attributes are allocated to each virtual gateway address:
Domain, which is the email domain name that is associated with the virtual gateway address, such as mycompany.com or mydomain.com.
IP address, which is the IPv4 or IPv6 address that is assigned to the virtual gateway address, such as 199.209.31.X or 2001:db8::X.
The other options are not attributes that are allocated to each virtual gateway address on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 5-14 and page 5-15.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118542-qa-esa- 00.html

QUESTION 43
When the Cisco ESA is configured to perform antivirus scanning, what is the default timeout value?

A. 30 seconds
B. 90 seconds
C. 60 seconds
D. 120 seconds

Correct Answer: C
Section:
Explanation:
When Cisco ESA is configured to perform antivirus scanning, the default timeout value is 60 seconds, which means that Cisco ESA will wait for 60 seconds for the antivirus engine to scan a message before applying the configured action for unscannable messages, such as deliver, drop, or quarantine.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 7-3.
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_chapter_01011.html

QUESTION 44
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: C
Section:
Explanation:
The global setting that is configured under Cisco ESA Scan Behavior is the actions for unscannable messages due to attachment type. This setting allows the administrator to specify what action to take when a message contains an attachment that cannot be scanned by the appliance, such as encrypted or password-protected files. The possible actions are:
Deliver - Deliver the message normally.
Drop - Drop the message silently without notifying the sender or recipient.
Quarantine - Quarantine the message in a specified policy quarantine.
Bounce - Bounce the message back to the sender with a specified reason.
Reference:
Scan Behavior
Reference: https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scanbehavior-impact-on-av/td-p/3923243

QUESTION 45

Which action on the Cisco ESA provides direct access to view the safelist/blocklist?

A. Show the SLBL cache on the CLI.
B. Monitor Incoming/Outgoing Listener.
C. Export the SLBL to a .csv file.
D. Debug the mail flow policy.

Correct Answer: C
Section:
Explanation:
The safelist/blocklist (SLBL) is a feature that allows Cisco ESA to accept or reject messages from specific email addresses or domains, based on the configuration of mail flow policies or end user preferences.
The action that provides direct access to view the SLBL on Cisco ESA is to export the SLBL to a .csv file, which can be done from the web user interface by selecting Security Services > Safelist/Blocklist and clicking Export.
The other options do not provide direct access to view the SLBL on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-13 and page 6-14.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117922-technote- esa-00.html

QUESTION 46
Which scenario prevents a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA?

A. A policy quarantine is missing.
B. More than one email pipeline is defined.
C. The "modify the message subject" is already set.
D. The "add custom header" action is performed first.

Correct Answer: A
Section:
Explanation:
A policy quarantine is a type of quarantine that allows Cisco ESA to store messages that match certain criteria, such as virus, spam, or DLP verdicts, for further review or release by an administrator or an end user.
A scenario that prevents a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA is when a policy quarantine is missing, which means that no policy quarantine has been created or enabled on Cisco ESA.
The other options do not prevent a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-2 and page 10-3.

QUESTION 47
What are two primary components of content filters? (Choose two.)

A. conditions
B. subject
C. content
D. actions
E. policies

Correct Answer: A, D
Section:
Explanation:
Content filters are rules that allow Cisco ESA to perform actions on messages based on predefined or custom conditions, such as headers, envelope, body, attachments, etc.
The two primary components of content filters are:
Conditions, which are the criteria that determine whether a message matches a content filter rule or not, such as message size, sender address, attachment type, etc.

Actions, which are the operations that Cisco ESA performs on a message if it matches the conditions of a content filter rule, such as deliver, drop, quarantine, encrypt, etc.
The other options are not primary components of content filters on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-3 and page 8-4.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_01010.pdf

QUESTION 48
A network administrator is modifying an outgoing mail policy to enable domain protection for the organization. A DNS entry is created that has the public key.
Which two headers will be used as matching criteria in the outgoing mail policy? (Choose two.)

A. message-ID
B. sender
C. URL reputation
D. from
E. mail-from

Correct Answer: B, D
Section:
Explanation:
To enable domain protection for the organization, the administrator must configure an outgoing mail policy that matches the sender and the from headers of the email. The sender header is the envelope sender address that is used by SMTP to route the email. The from header is the address that is displayed to the recipient as the source of the email. These headers are used to generate and verify a DomainKeys Identified Mail (DKIM) signature, which is a cryptographic method of validating the authenticity and integrity of an email message.
The other headers are not relevant for domain protection. The message-ID header is a unique identifier for each email message. The URL reputation header is a score that indicates the likelihood of a URL being malicious. The mail-from header is an alias for the sender header.
Reference:
Domain Protection
DKIM Signing

QUESTION 49
To comply with a recent audit, an engineer must configure anti-virus message handling options on the incoming mail policies to attach warnings to the subject of an email.
What should be configured to meet this requirement for known viral emails?

A. Virus Infected Messages
B. Unscannable Messages
C. Encrypted Messages
D. Positively Identified Messages

Correct Answer: A
Section:
Explanation:
Message Handling Settings:
Repaired Message Handling Messages are considered repaired if the message was completely scanned and all viruses have been repaired or removed. These messages will be delivered as is.
Encrypted Message Handling
Messages are considered encrypted if the engine is unable to finish the scan due to an encrypted or protected field in the message. Messages that are marked encrypted may also be repaired.
Unscannable Message Handling Messages are considered unscannable if a scanning timeout value has been reached, or the engine becomes unavailable due to an internal error. Messages that are marked unscannable may also be repaired.
Virus Infected Message Handling The system may be unable to drop the attachment or completely repair a message. In these cases, you can configure how the system handles messages that could still contain viruses.
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_chapter_01011.html#con_1132282

QUESTION 50

An administrator is managing multiple Cisco ESA devices and wants to view the quarantine emails from all devices in a central location.
How is this accomplished?

A. Disable the VOF feature before sending SPAM to the external quarantine.

B. Configure a mail policy to determine whether the message is sent to the local or external quarantine.

C. Disable the local quarantine before sending SPAM to the external quarantine.

D. Configure a user policy to determine whether the message is sent to the local or external quarantine.

Correct Answer: C
Section:
Explanation:

Disabling the Local Spam Quarantine to Activate the External Quarantine If you were using a local spam quarantine before enabling an external spam quarantine, you must disable the local quarantine in order to send messages to the external quarantine.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_0101010.html?bookSearch=true#con_1172419

QUESTION 51

A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy.
What is the reason of this?

A. The Tram* header is checked against all policies in a top-down fashion.

B. The message header with the highest priority is checked against each policy in a top-down fashion.

C. The To" header is checked against all policies in a top-down fashion.

D. The message header with the highest priority is checked against the Default policy in a top-down fashion.

Correct Answer: B
Section:
Explanation:

The envelope sender and the envelope recipeint have a higher priority over the sender header when you match a message to a mail policy. If you configure a mail policy to match a specific user, the messages are automatically classified into the mail policy based on the envelope sender and the envelope recipient. https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01001.html

QUESTION 52

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
Section:
Explanation:

The appliance enforces your organization's policies for messages sent to and from your users through the use of mail policies. These are sets of rules that specify the types of suspect, sensitive, or malicious content that your organization may not want entering or leaving your network. This content may include:
-spam

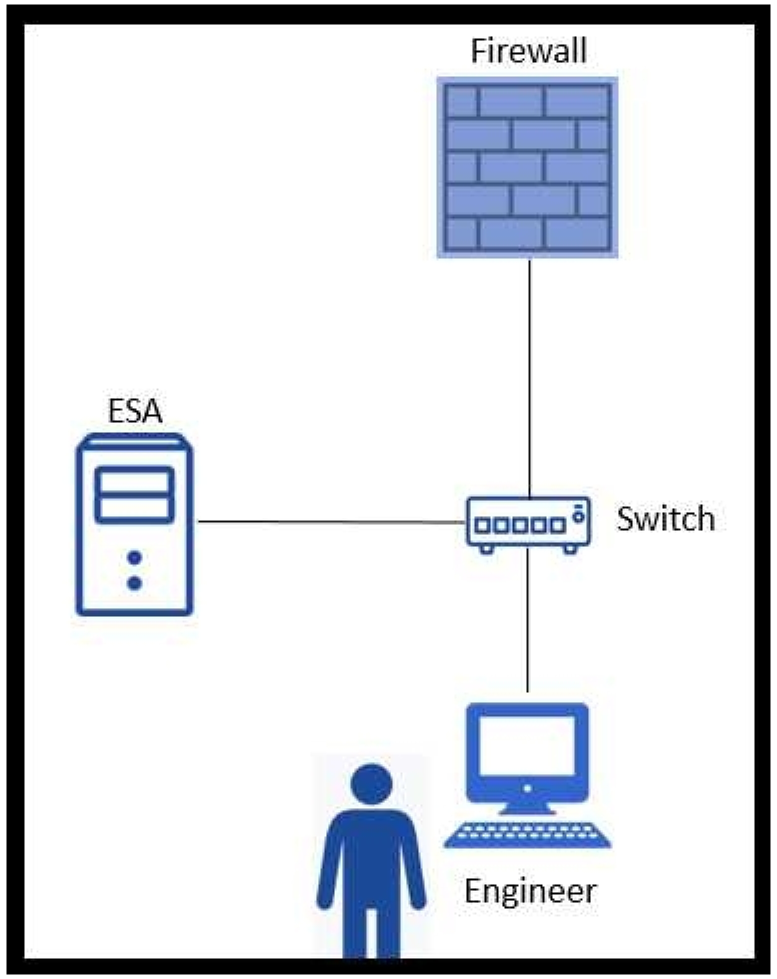
-legitimate marketing messages
-graymail
-viruses
-phishing and other targeted mail attacks
-confidential corporate data
-personally identifiable information
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01001.html?bookSearch=true

QUESTION 53
An engineer is testing mail flow on a new Cisco ESA and notices that messages for domain abc.com are stuck in the delivery queue. Upon further investigation, the engineer notices that the messages pending delivery are destined for 192.168.1.11, when they should instead be routed to 192.168.1.10.
What configuration change needed to address this issue?

A. Add an address list for domain abc.com.
B. Modify Destination Controls entry for the domain abc.com.
C. Modify the SMTP route for the domain and change the IP address to 192.168.1.10.
D. Modify the Routing Tables and add a route for IP address to 192.168.1.10.

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html
You can use the SMTP route feature on Cisco ESA to specify how messages for a specific domain are routed to their destination. You can modify the SMTP route for the domain abc.com and change the IP address to 192.168.1.10 to ensure that messages are delivered correctly3. Reference = Securing Email with Cisco Email Security Appliance (SESA) v3.1

QUESTION 54

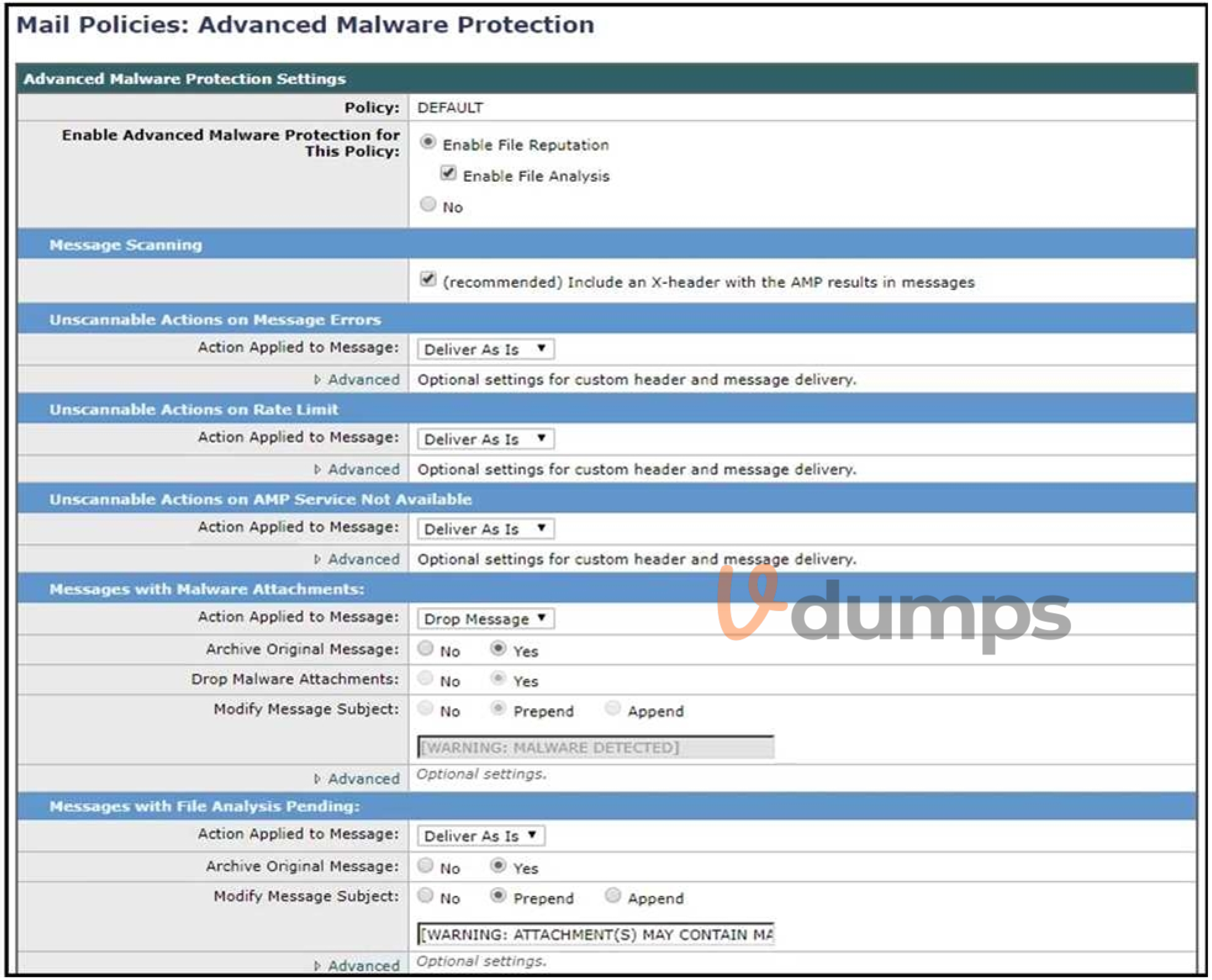


Refer to the exhibit. An engineer is trying to connect to a Cisco ESA using SSH and has been unsuccessful. Upon further inspection, the engineer notices that there is a loss of connectivity to the neighboring switch. Which connection method should be used to determine the configuration issue?

A. Telnet
B. HTTPS
C. Ethernet
D. serial

Correct Answer: D
Section:
Explanation:
Serial connection is a method that should be used to determine the configuration issue when there is a loss of connectivity to the neighboring switch. Serial connection allows the engineer to access the Cisco ESA console port using a serial cable and a terminal emulator, such as PuTTY or HyperTerminal, without relying on the network connectivity.
The other options are not valid methods to determine the configuration issue when there is a loss of connectivity to the neighboring switch, because they require network connectivity to work.
Reference: Cisco Email Security Appliance C690 Quickstart Guide, page 2.

QUESTION 55



Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings

Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	● Enable File Reputation ☑ Enable File Analysis ○ No

Message Scanning

☑ (recommended) Include an X-header with the AMP results in messages

Unscannable Actions on Message Errors

Action Applied to Message:	Deliver As Is ▼
▹ Advanced	Optional settings for custom header and message delivery.

Unscannable Actions on Rate Limit

Action Applied to Message:	Deliver As Is ▼
▹ Advanced	Optional settings for custom header and message delivery.

Unscannable Actions on AMP Service Not Available

Action Applied to Message:	Deliver As Is ▼
▹ Advanced	Optional settings for custom header and message delivery.

Messages with Malware Attachments:

Action Applied to Message:	Drop Message ▼
Archive Original Message:	○ No ● Yes
Drop Malware Attachments:	○ No ● Yes
Modify Message Subject:	○ No ● Prepend ○ Append [WARNING: MALWARE DETECTED]
▹ Advanced	*Optional settings.*

Messages with File Analysis Pending:

Action Applied to Message:	Deliver As Is ▼
Archive Original Message:	○ No ● Yes
Modify Message Subject:	○ No ● Prepend ○ Append [WARNING: ATTACHMENT(S) MAY CONTAIN MA
▹ Advanced	*Optional settings.*

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: B
Section:

Explanation:
Overview of File Reputation Filtering and File Analysis:
Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:
-Obtaining the reputation of known files.
-Analyzing behavior of certain files that are not yet known to the reputation service.
-Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.
-This feature is available for incoming messages and outgoing messages.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_010000.html?bookSearch=true

QUESTION 56
Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?

A. Set up the interface group with the flag.
B. Issue the altsrchost command.
C. Map the envelope sender address to the host.
D. Apply a filter on the message.

Correct Answer: D
Section:
Explanation:
A filter is a method that enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way. A filter is a rule that allows Cisco ESA to perform actions on messages based on predefined or custom conditions, such as headers, envelope, body, attachments, etc.
To deliver a flagged message to a specific virtual gateway address using a filter, the engineer can create a content filter or message filter that matches the flag condition and applies an action of "deliver via alternate host" with the virtual gateway address as the parameter.
The other options are not methods that enable an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way, because they have more limitations or requirements than using a filter.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-3 and page 8-7.

QUESTION 57
A Cisco ESA administrator was notified that a user was not receiving emails from a specific domain.
After reviewing the mail logs, the sender had a negative sender-based reputation score.
What should the administrator do to allow inbound email from that specific domain?

A. Create a new inbound mail policy with a message filter that overrides Talos.
B. Ask the user to add the sender to the email application's allow list.
C. Modify the firewall to allow emails from the domain.
D. Add the domain into the allow list.

Correct Answer: D
Section:
Explanation:
The allow list is a feature that allows Cisco ESA to accept messages from specific email addresses or domains, regardless of their sender-based reputation score or other reputation filters.
To allow inbound email from that specific domain, the administrator should add the domain into the allow list on Cisco ESA, which can be done from the web user interface by selecting Security Services > Safelist/Blocklist and clicking Add Entry.
The other options are not valid solutions to allow inbound email from that specific domain, because they do not affect the sender-based reputation score or the reputation filters on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-13 and page 6-14.

QUESTION 58
An email containing a URL passes through the Cisco ESA that has content filtering disabled for all mail policies. The sender is sampleuser@test1.com, the recipients are testuser1@test2.com, testuser2@test2.com, testuser3@test2.com, and mailer1@test2.com. The subject of the email is Test Document395898847. An administrator wants to add a policy to ensure that the Cisco ESA evaluates the web reputation score before permitting

this email.
Which two criteria must be used by the administrator to achieve this? (Choose two.)

A. Subject contains Test Document"
B. Sender matches test1.com
C. Email body contains a URL
D. Date and time of email
E. Email does not match mailer1@test2.com

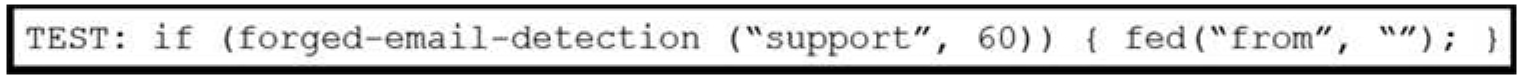
Correct Answer: B, C
Section:
Explanation:
Web reputation score is a feature that allows Cisco ESA to evaluate the reputation of URLs in messages based on real-time data from Talos intelligence and apply appropriate actions, such as block, quarantine, or deliver.
To ensure that Cisco ESA evaluates the web reputation score before permitting this email, the administrator should use two criteria to create a content filter or message filter that matches this email and applies an action of "check web reputation":
Sender matches test1.com, which means that the sender's domain name is test1.com.
Email body contains a URL, which means that the message body has one or more URLs in it.
The other options are not valid criteria to ensure that Cisco ESA evaluates the web reputation score before permitting this email, because they do not match this email or they are not relevant to web reputation score.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-3 and page 8-7.

QUESTION 59
A recent engine update was pulled down for graymail and has caused the service to start crashing. It is critical to fix this as quickly as possible.
What must be done to address this issue?

A. Roll back to a previous version of the engine from the Services Overview page.
B. Roll back to a previous version of the engine from the System Health page.
C. Download another update from the IMS and Graymail page.
D. Download another update from the Service Updates page.

Correct Answer: A
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_0100010.html#task_9F07A032042F48C6AEDB69D325CD3C5F
To address this issue, the administrator should roll back to a previous version of the engine from the Services Overview page on Cisco ESA. This will restore the functionality of graymail service and prevent it from crashing.
The Services Overview page allows the administrator to view and manage various services on Cisco ESA, such as antivirus, outbreak filters, graymail, etc., and perform actions such as enable/disable, update, or roll back.
The other options are not valid solutions to address this issue, because they do not allow the administrator to roll back to a previous version of the engine for graymail service.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-18 and page 6-19.

QUESTION 60



```
TEST: if (forged-email-detection (“support”, 60)) { fed(“from”, “”); }
```

Refer to the exhibit. An engineer needs to change the existing Forged Email Detection message filter so that it references a newly created dictionary named 'Executives'.
What should be done to accomplish this task?

A. Change "from" to "Executives".
B. Change "TESF to "Executives".
C. Change fed' to "Executives".
D. Change "support" to "Executives".

Correct Answer: D
Section:
Explanation:
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKSEC-2240.pdf

QUESTION 61
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
Section:
Explanation:
Modify Subject is an additional option that should be used to help the end users be aware of the elevated risk of interacting with these messages. Modify Subject allows the administrator to add a prefix or suffix to the message subject, such as "[SPF Fail]", to indicate that the message has failed the SPF verification and may be fraudulent or spoofed.
The other options are not valid additional options to help the end users be aware of the elevated risk of interacting with these messages, because they do not affect the message subject or provide any warning to the end users.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-7 and page 8-8.

QUESTION 62
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?

A. Outgoing Mail Policy
B. Preliminary Mail Policy
C. Incoming Mail Flow Policy
D. Outgoing Mail Flow Policy

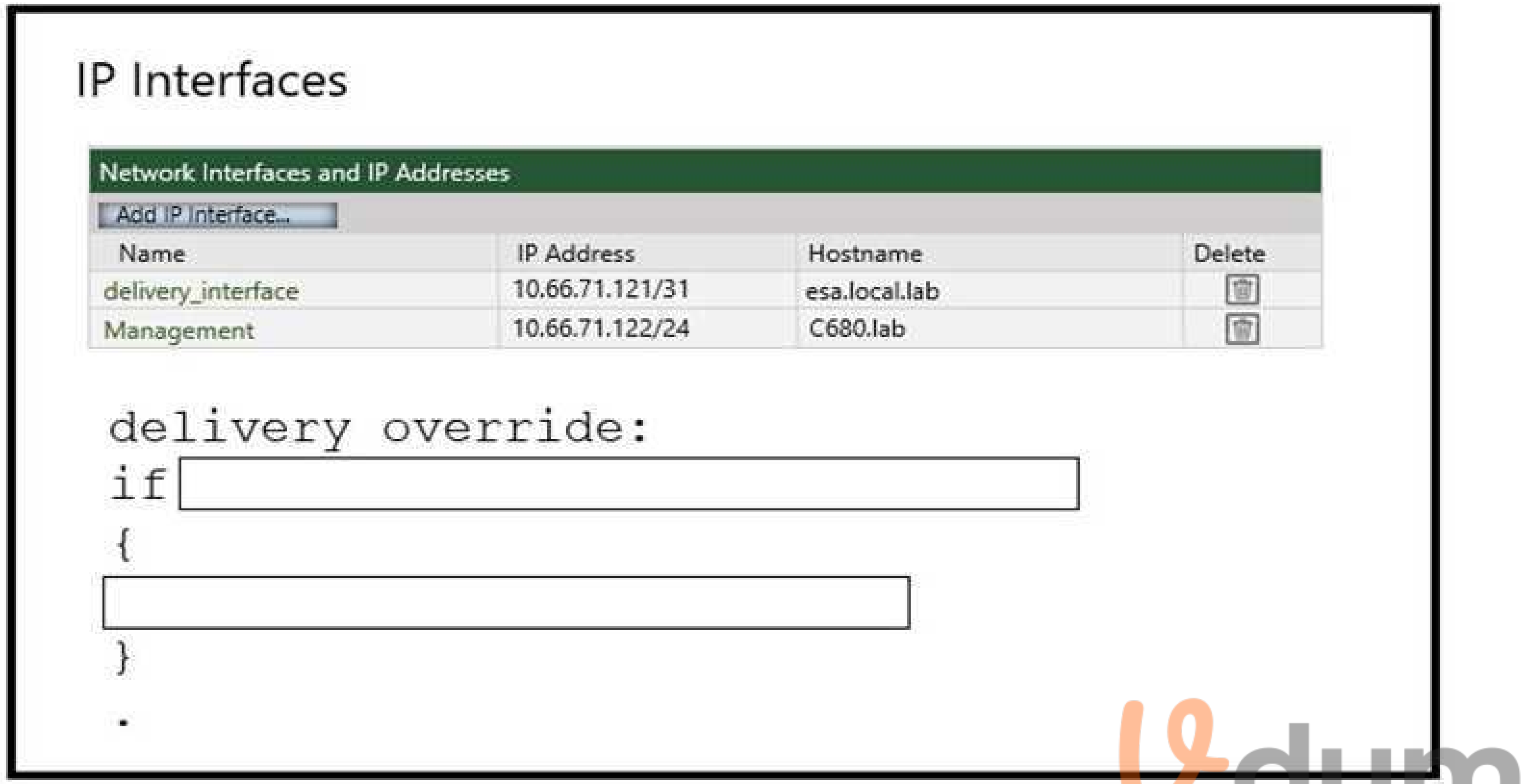
Correct Answer: A
Section:
Explanation:
Outgoing Mail Policy is a mail policy that should be created to accomplish this task. Outgoing Mail Policy is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.
To create an Outgoing Mail 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.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2 and page 9-4.

QUESTION 63

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:



IP Interfaces

Network Interfaces and IP Addresses

Name	IP Address	Hostname	Delete
delivery_interface	10.66.71.121/31	esa.local.lab	🗑
Management	10.66.71.122/24	C680.lab	🗑

```
delivery override:
if [                              ]
{
[                              ]
}
.
```

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

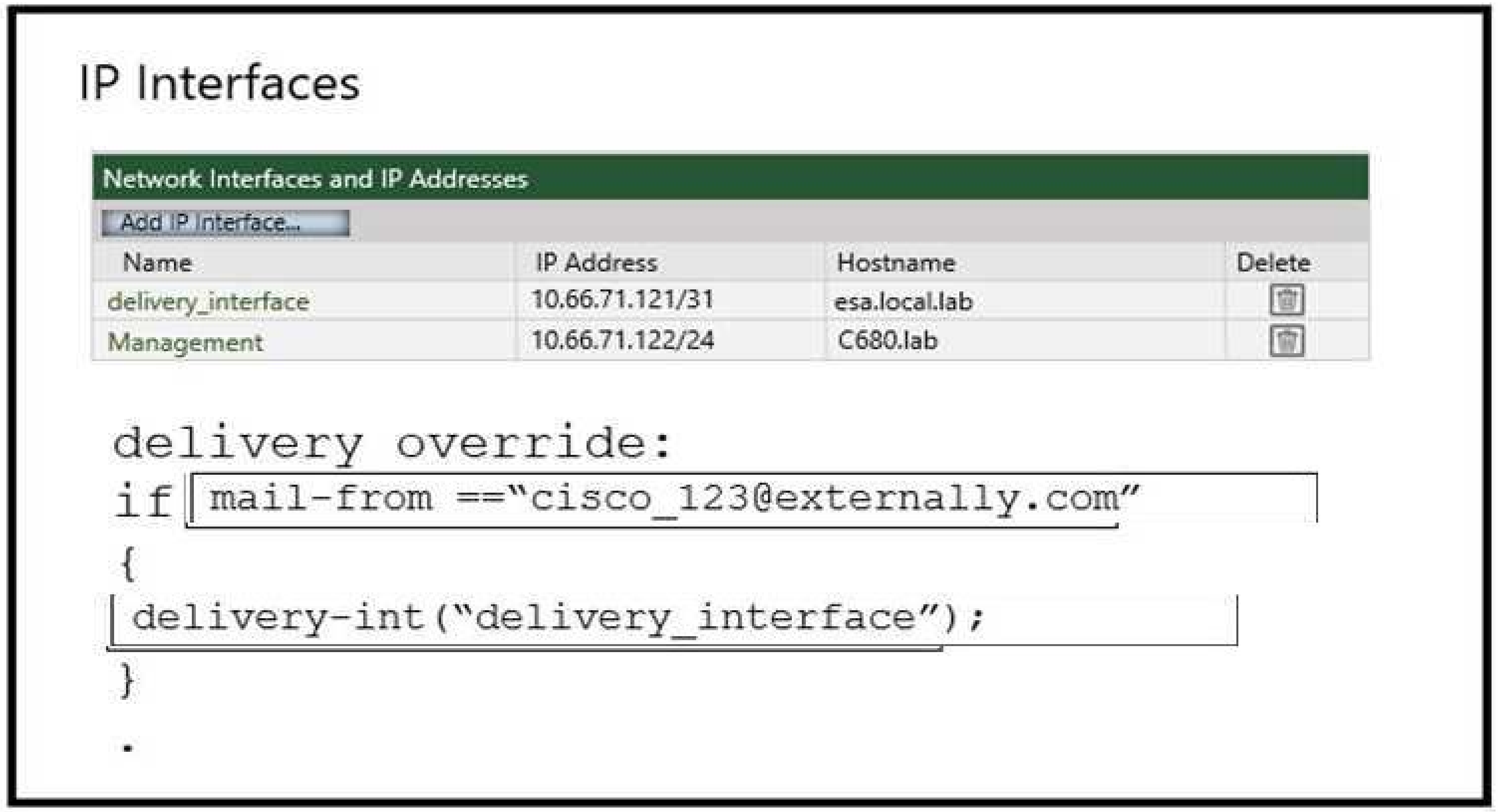
```
mail-from ==“cisco_123@externally.com”
```

```
Sender ==“cisco_123@externally.com
```

```
delivery-int(“delivery_interface”);
```

```
alt-src-host(“delivery_interface”);
```

Correct Answer:



IP Interfaces

Network Interfaces and IP Addresses

Name	IP Address	Hostname	Delete
delivery_interface	10.66.71.121/31	esa.local.lab	🗑
Management	10.66.71.122/24	C680.lab	🗑

```
delivery override:
if  mail-from =="cisco_123@externally.com"
{
delivery-int("delivery_interface");
}
.
```

```
Envelope-sender =="cisco_123@externally.com"
```

```
Sender =="cisco_123@externally.com
```

```
alt-src-host("delivery_interface");
```

Section:
Explanation:

QUESTION 64
Which component must be added to the content filter to trigger on failed SPF Verification or DKIM Authentication verdicts?

A. status
B. response
C. parameter
D. condition

Correct Answer: D
Section:
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.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 8-3 and page 8-4.

QUESTION 65
An organization wants to use DMARC to improve its brand reputation by leveraging DNS records.
Which two email authentication mechanisms are utilized during this process? (Choose two.)

A. SPF
B. DSTP
C. DKIM
D. TLS
E. PKI

Correct Answer: A, C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/products/security/what-is-dmarc.html
SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) are two email authentication mechanisms that are utilized during this process. SPF and DKIM allow the domain owner to publish DNS records that specify the authorized IP addresses or hosts for sending emails from that domain and sign the messages with a cryptographic key to prove their authenticity and integrity.
DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication standard that builds on SPF and DKIM and allows the domain owner to publish DNS records that specify how receivers should handle messages that fail SPF or DKIM verification, such as reject, quarantine, or none, and how to report back the results of DMARC validation.
The other options are not valid email authentication mechanisms that are utilized during this process, because they are not part of DMARC standard.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 11-2 and page 11-3.

QUESTION 66
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: B
Section:
Explanation:
SPF verification is a feature that allows Cisco ESA to verify the authenticity of the sender's domain by checking the sender's IP address against a DNS record published by the domain owner. An SPF record is a TXT record that specifies the authorized IP addresses or hosts for sending emails from a domain, using a syntax of qualifiers, mechanisms, and modifiers.
The reason why the verification is not working properly is that SPF verification is disabled on the mail flow policy that applies to the messages sent from domain abc.com. A mail flow policy is a set of rules that determine how incoming or outgoing messages are processed by Cisco ESA, including whether to enable SPF verification or not.
To enable SPF verification on the mail flow policy, the administrator can follow these steps:
Select Mail Policies > Mail Flow Policies and click Edit Settings for the mail flow policy that applies to the messages sent from domain abc.com.

Under Sender Authentication, select Enable SPF Verification and choose an SPF conformance level from the drop-down menu.
Click Submit.
The other options are not valid reasons why the verification is not working properly, because they do not affect SPF verification on the mail flow policy.

QUESTION 67
An administrator needs to configure Cisco ESA to ensure that emails are sent and authorized by the owner of the domain. Which two steps must be performed to accomplish this task? (Choose two.)

A. Generate keys.
B. Create signing profile.
C. Create Mx record.
D. Enable SPF verification.
E. Create DMARC profile.

Correct Answer: A, B
Section:
Explanation:
Configuring DomainKeys and DKIM Signing:
-Signing Keys
-Public Keys
-Domain Profiles
Creating Domain Profiles:
Step 1
-Choose Mail Policies > Signing Profiles.
Step 2
-In the Domain Signing Profiles section, click Add Profile.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_010110.html?bookSearch=true

QUESTION 68
What is the purpose of Cisco Email Encryption on Cisco ESA?

A. to ensure anonymity between a recipient and MTA
B. to ensure integrity between a sender and MTA
C. to authenticate direct communication between a sender and Cisco ESA
D. to ensure privacy between Cisco ESA and MTA

Correct Answer: D
Section:
Explanation:
Overview of Encrypting Communication with Other MTAs:
AsyncOS supports the STARTTLS extension to SMTP (Secure SMTP over TLS).
The TLS implementation in AsyncOS provides privacy through encryption.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_011001.html?bookSearch=true

QUESTION 69
A Cisco ESA administrator has noticed that new messages being sent to the Centralized Policy
Quarantine are being released after one hour. Previously, they were being held for a day before being released.
What was configured that caused this to occur?

A. The retention period was changed to one hour.
B. The threshold settings were set to override the clock settings.
C. The retention period was set to default.
D. The threshold settings were set to default.

Correct Answer: C
Section:
Explanation:
You can configure Policy, Virus, and Outbreak Quarantines in any one of the following ways:
Choose Quarantine > Other Quarantine > View > +.
Choose Monitor > Policy, Virus, and Outbreak Quarantines and do one of the following.
Click Add Policy Quarantine.
Keep the following in mind, changing the retention time of the File Analysis quarantine from the default of one hour is not recommended.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_011111.html?bookSearch=true

QUESTION 70
What are organizations trying to address when implementing a SPAM quarantine?

A. true positives
B. false negatives
C. false positives
D. true negatives

Correct Answer: C
Section:
Explanation:
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_0100000.html#con_1482874
False positives are legitimate messages that are incorrectly identified as spam by the Cisco ESA. Organizations may want to implement a spam quarantine to reduce the risk of losing false positive messages and allow users or administrators to review and release them2. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Spam
Quarantine [Cisco Secure Email Gateway] - Cisco

QUESTION 71
Which two Cisco ESA features are used to control email delivery based on the sender? (Choose two.)

A. incoming mail policies
B. spam quarantine
C. outbreak filter
D. safelists
E. blocklists

Correct Answer: D, E
Section:
Explanation:
Safelists and blocklists are features on Cisco ESA that allow you to control email delivery based on the sender. Safelists are lists of sender addresses or domains that you want to accept or exempt from certain filtering actions. Blocklists are lists of sender addresses or domains that you want to reject or drop3. Reference = Securing Email with Cisco Email Security Appliance (SESA) v3.1

QUESTION 72

What is the purpose of checking the CRL during SMTP authentication on a Cisco Secure Email Gateway?

A. Validate the date to check if the certificate is still valid
B. Check if the certificate is not revoked.
C. Confirm that corresponding CA is present
D. Verify the common name matches user ID

Correct Answer: B
Section:
Explanation:
The purpose of checking the Certificate Revocation List (CRL) during SMTP authentication on a Cisco
Secure Email Gateway is to check if the certificate is not revoked by the issuing Certificate Authority (CA). A revoked certificate means that it is no longer valid and should not be trusted. Reference = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) -Configuring SMTP Authentication [Cisco Secure Email Gateway] - Cisco]

QUESTION 73
An organization wants to designate help desk personnel to assist with tickets that request the release of messages from the spam quarantine because company policy does not permit direct end-user access to the quarantine. Which two roles must be used to allow help desk personnel to release messages while restricting their access to make configuration changes in the Cisco Secure Email Gateway? (Choose two.)

A. Administrator
B. Help Desk User
C. Read-Only Operator
D. Technician
E. Quarantine Administrator

Correct Answer: B, E
Section:
Explanation:
All users with administrator privileges can change spam quarantine settings and view and manage messages in the spam quarantine. You do not need to configure spam quarantine access for administrator users.
If you configure access to the spam quarantine for users with the following roles, they can view, release, and delete messages in the spam quarantine:
-Operator
-Read-only operator
-Help desk user
-Guest
-Custom user roles that have spam quarantine privileges
These users cannot access spam quarantine settings.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_0100000.html?bookSearch=true#con_1624156

QUESTION 74
When the spam quarantine is configured on the Cisco Secure Email Gateway, which type of query is used to validate non administrative user access to the end-user quarantine via LDAP?

A. spam quarantine end-user authentication
B. spam quarantine alias consolidation
C. spam quarantine external authorization
D. local mailbox (IMAP/POP) authentication

Correct Answer: A
Section:
Explanation:

spam quarantine end-user authentication query is used to validate non administrative user access to the end-user quarantine via LDAP1. This query is configured in the System Administration > LDAP > LDAP Server Profile page and can be tested using the smtproutes command in the CLI1. The other queries are not related to this task. The spam quarantine alias consolidation query is used to consolidate multiple email addresses for a user into one login2. The spam quarantine external authorization query is used to authorize users to access an external spam quarantine on a separate Cisco Secure Email and Web Manager3. The local mailbox (IMAP/POP) authentication is an alternative method to authenticate users without using LDAP2.

QUESTION 75
An administrator notices that incoming emails with certain attachments do not get delivered to all recipients when the emails have multiple recipients in different domains like cisco.com and test.com.
The same emails when sent only to recipients in cisco.com are delivered properly. How must the Cisco Secure Email Gateway be configured to avoid this behavior?

A. Modify mail policies for cisco.com to ensure that emails are not dropped.
B. Modify mail policies so email recipients do not match multiple policies.
C. Modify DLP configuration to ensure that all attachments are permitted for test.com.
D. Modify DLP configuration to exempt DLP scanning for messages sent to test.com domain

Correct Answer: B
Section:
Explanation:
By modifying the mail policies, specifically the recipient matching criteria, you can ensure that email recipients do not match multiple policies simultaneously. When recipients in the email message belong to different domains (e.g., cisco.com and test.com), it can result in multiple policies being triggered simultaneously, leading to inconsistent delivery of emails with attachments.
DLP is for outgoing mail only and not relevant to incoming mail.

QUESTION 76
An engineer is tasked with creating a content filter to catch attachments, including credit card numbers, and hold them for review until further action is taken. Which component on a Cisco Secure Email Gateway must be configured to meet this requirement?

A. Spam Quarantine
B. Policy Quarantine
C. Outbreak Filter
D. Content Filter

Correct Answer: D
Section:
Explanation:
Content filter is a component on a Cisco Secure Email Gateway that must be configured to catch attachments, including credit card numbers, and hold them for review until further action is taken.
Content filter allows you to define rules based on message content and apply actions such as quarantine, encrypt, or modify. Reference = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Content Filters [Cisco Secure Email Gateway] - Cisco]

QUESTION 77
Which of the following two steps are required to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance? (Choose two.)

A. Paste in the Registration Token generated from the Smart Licensing Account
B. Enable the Threat Response service under Network>Cloud Service Settings.
C. Select the correct Threat Response Server based on your region.
D. Paste in the Registration Token generated from the Security Services Exchange.
E. Enable the Security Services Exchange service under Network>Cloud Service Settings

Correct Answer: B, C
Section:

Explanation:
one of the methods to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance is to use the Threat Response service1. This service allows the appliance to send telemetry data to the SecureX cloud and provide visibility and response capabilities across multiple security products1. To use this service, the administrator needs to perform the following steps1:
Enable the Threat Response service: The administrator needs to go to Network > Cloud Service Settings and enable the Threat Response service. This will generate a registration token that can be used to register the appliance with SecureX1.
Select the correct Threat Response Server: The administrator needs to select the appropriate Threat Response server based on the region where the appliance is located. The available regions are North America, Europe, and Asia Pacific1.

QUESTION 78
What are the two different phases in the process of Cisco Secure Email Gateway performing S/MIME encryption? (Choose two.)

A. Attach the encrypted public key to the message
B. Encrypt the message body using the session key
C. Send the encrypted message to the sender
D. Attach the encrypted symmetric key to the message
E. Create a pseudo-random session key.

Correct Answer: D, E
Section:

QUESTION 79
A Cisco Secure Email Gateway administrator is creating a Mail Flow Policy to receive outbound email from Microsoft Exchange. Which Connection Behavior must be selected to properly process the messages?

A. Accept
B. Delay
C. Relay
D. Reject

Correct Answer: C
Section:
Explanation:
Relay is the connection behavior that must be selected to properly process the messages. Relay allows Cisco ESA to accept messages from the specified source and deliver them to the intended destination, without applying any content or reputation filters.
To configure a mail flow policy with relay connection behavior on Cisco ESA, the administrator can follow these steps:
Select Mail Policies > Mail Flow Policies and click Add Policy.
Enter a name and description for the mail flow policy, such as Exchange Outbound.
Under Connection Behavior, select Relay.
Click Submit.
The other options are not valid connection behaviors to properly process the messages, because they either reject, delay, or accept the messages with content or reputation filters applied.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 6-2 and page 6-3.

QUESTION 80
An organization wants to prevent proprietary patent documents from being shared externally via email. The network administrator reviewed the DLP policies on the Cisco Secure Email Gateway and could not find an existing policy with the appropriate matching patterns. Which type of DLP policy template must be used to create a policy that meets this requirement?

A. privacy protection
B. custom policy
C. regulatory compliance

D. acceptable use

Correct Answer: B
Section:
Explanation:
Custom policy is a type of DLP policy template that must be used to create a policy that meets this requirement. Custom policy allows the administrator to define their own criteria for detecting sensitive or confidential data in messages, such as keywords, regular expressions, file types, etc.
To create a custom DLP policy on Cisco ESA, the administrator can follow these steps:
Select Mail Policies > DLP Policy Manager and click Add Policy.
Enter a name and description for the DLP policy, such as Patent Protection.
Under Policy Template, select Custom Policy.
Click Submit.
Under Content Matching Criteria, click Add Criteria.
Choose a matching type, such as Keyword or Regular Expression, and enter a value that matches the proprietary patent documents, such as "patent number" or "\d{4}/\d{6}".
Click Submit.
The other options are not valid types of DLP policy templates to create a policy that meets this requirement, because they are predefined templates that do not match the proprietary patent documents.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 9-3 and page 9-5.

QUESTION 81
When a network engineer is troubleshooting a mail flow issue, they discover that some emails are rejected with an SMTP code of 451 and the error message "#4.7.1 Unable to perform DMARC verification". In the DMARC verification profile on the Cisco Secure Email Gateway appliance, which action must be set for messages that result in temporary failure to prevent these emails from being rejected?

A. Accept
B. Ignore
C. Quarantine
D. No Action

Correct Answer: A
Section:
Explanation:
Accept is the action that must be set for messages that result in temporary failure to prevent these emails from being rejected. Accept allows Cisco ESA to deliver the messages without applying any DMARC actions or modifications.
To configure the accept action for messages that result in temporary failure on Cisco ESA, the administrator can follow these steps:
Select Mail Policies > DMARC Verification Profile and click Edit Settings for the DMARC verification profile that applies to the messages.
Under DMARC Actions, select Accept from the drop-down menu for Messages That Result in Temporary Failure.
Click Submit.
The other options are not valid actions for messages that result in temporary failure to prevent these emails from being rejected, because they either apply DMARC actions or modifications or do nothing.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 11-4 and page 11-5.

QUESTION 82
A network engineer must tighten up the SPAM control policy of an organization due to a recent SPAM attack. In which scenario does enabling regional scanning improve security for this organization?

A. when most of the received spam comes from a specific country
B. when most of the received spam originates outside of the U.S.
C. when most of the received email originates outside of the U.S.
D. when most of the received email originates from a specific region

Correct Answer: D
Section:

Explanation:

Enabling regional scanning improves security for this organization when most of the received email originates from a specific region. Regional scanning is a feature that allows Cisco ESA to apply different spam thresholds and actions based on the geographic region of the sender's IP address, using a database of IP addresses and regions.

To enable regional scanning on Cisco ESA, the administrator can follow these steps:

Select Security Services > IronPort Anti-Spam and click Edit Settings.

Under Regional Scanning, select Enable Regional Scanning.

Click Submit.

Select Security Services > IronPort Anti-Spam > Regional Settings and click Add Region.

Choose a region from the drop-down menu, such as Asia Pacific.

Enter a spam threshold and an action for that region, such as 80 and Drop.

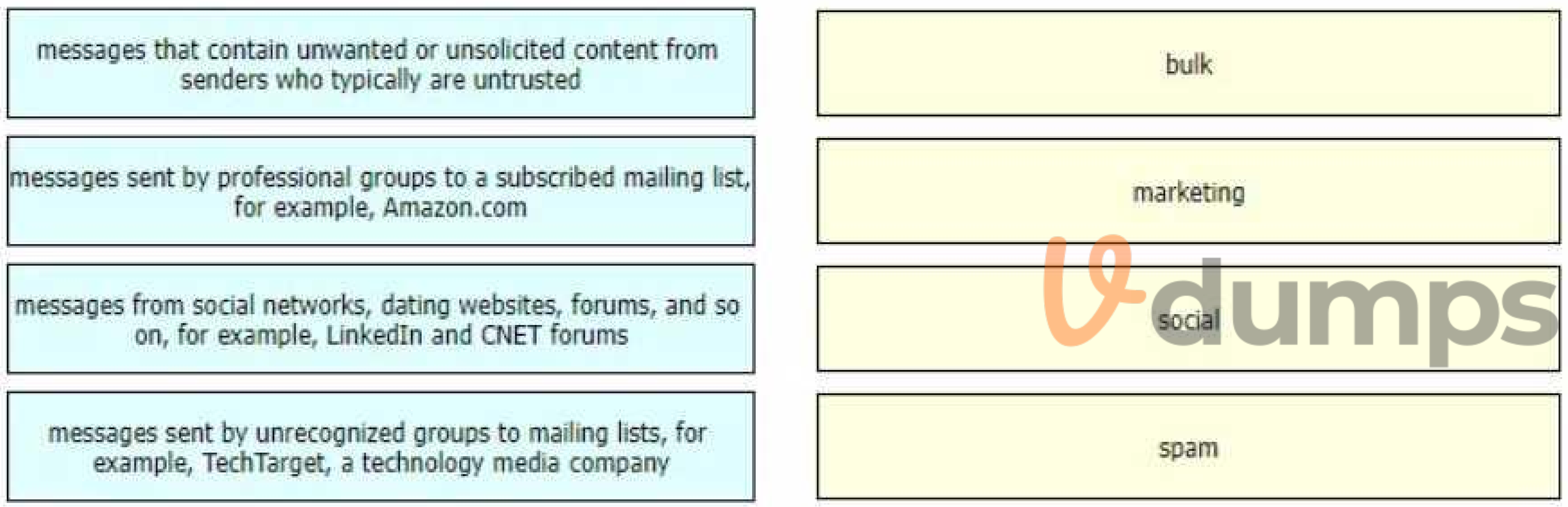
Click Submit.

QUESTION 83

DRAG DROP

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

Select and Place:



messages that contain unwanted or unsolicited content from senders who typically are untrusted

messages sent by professional groups to a subscribed mailing list, for example, Amazon.com

messages from social networks, dating websites, forums, and so on, for example, LinkedIn and CNET forums

messages sent by unrecognized groups to mailing lists, for example, TechTarget, a technology media company

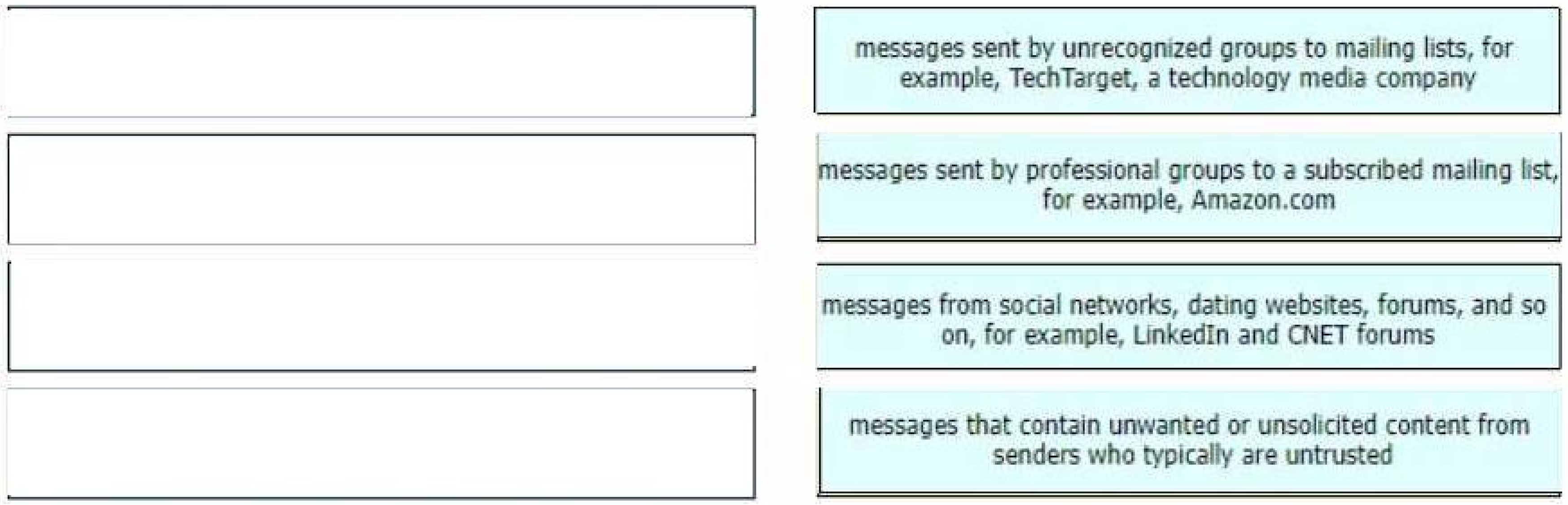
bulk

marketing

social

spam

Correct Answer:



messages sent by unrecognized groups to mailing lists, for example, TechTarget, a technology media company

messages sent by professional groups to a subscribed mailing list, for example, Amazon.com

messages from social networks, dating websites, forums, and so on, for example, LinkedIn and CNET forums

messages that contain unwanted or unsolicited content from senders who typically are untrusted

Section:

Explanation:

QUESTION 84

A content dictionary was created for use with Forged Email Detection. Proper data that pertains to the CEO Example CEO: <ceo@example com> must be entered. What must be added to the dictionary to accomplish this goal?

A. example.com

B. Example CEO

C. ceo

D. ceo@example com

Correct Answer: D
Section:
Explanation:
ceo@example.com is the data that must be added to the dictionary to accomplish this goal. A content dictionary is a list of values that can be used as a condition in a content filter or a message filter. Forged Email Detection is a feature that allows Cisco ESA to detect and prevent email spoofing attacks, where the sender's address or domain is forged to appear as someone else, such as the CEO of the organization.
To create a content dictionary for use with Forged Email Detection on Cisco ESA, the administrator can follow these steps:
Select Mail Policies > Content Dictionaries and click Add Dictionary.
Enter a name and description for the content dictionary, such as CEO Email.
Under Dictionary Values, click Add Value.
Enter the email address of the CEO, such as ceo@example.com.
Click Submit.

QUESTION 85

A security administrator deployed a Cisco Secure Email Gateway appliance with a mail policy configured to store suspected spam for review. The appliance is the DMZ and only the standard HTTP/HTTPS ports are allowed by the firewall. An administrator wants to ensure that users can view any suspected spam that was blocked. Which action must be taken to meet this requirement?

A. Enable the external Spam Quarantine and enter the IP address and port for the Secure Email and Web Manager

B. Enable the Spam Quarantine and leave the default settings unchanged.

C. Enable End-User Quarantine Access and point to an LDAP server for authentication.

D. Enable the Spam Quarantine and specify port 80 for HTTP and port 443 for HTTPS

Correct Answer: C
Section:
Explanation:
Enabling End-User Quarantine Access and pointing to an LDAP server for authentication is the action that must be taken to meet this requirement. End-User Quarantine Access is a feature that allows users to access their personal quarantine on Cisco ESA using their email address and password, without requiring an administrator account or access to Secure Email and Web Manager.
To enable End-User Quarantine Access on Cisco ESA, the administrator can follow these steps:
Select Security Services > IronPort Anti-Spam > End User Safelist/Blocklist Settings and click Edit Settings.
Under End User Quarantine Access, select Enable End User Quarantine Access.
Under Authentication Server, select LDAP Server from the drop-down menu and choose an LDAP server profile from the drop-down menu.
Click Submit.

QUESTION 86

Which of the following two statements are correct about the large file attachments (greater than 25MB) feature in Cisco Secure Email Encryption Service? (Choose two.)

A. Large file attachments can only be sent using the websafe portal

B. This feature allows users to send up to 50MB of attachments in a secure email.

C. Large file attachments will be sent as a securedoc attachment

D. Large file attachments can only be sent using the Cisco Secure Email Add-In.

E. This feature can only be enabled if the Read from Message feature is enabled

Correct Answer: C, E
Section:
Explanation:
Large file attachments will be sent as a securedoc attachment. This means that the recipient will receive an encrypted message with a securedoc.html attachment that contains a link to download the large file from the Cisco Secure Email Encryption Service portal[2, p. 9].
This feature can only be enabled if the Read from Message feature is enabled. The Read from Message feature allows you to encrypt messages based on keywords or phrases in the subject or body of the message. You need to enable this feature before you can enable the large file attachments feature[2, p. 8].
The other options are not valid because:
A. Large file attachments can be sent using both the websafe portal and the Cisco Secure Email Add-In. The websafe portal allows you to compose and send encrypted messages from any web browser, while the Cisco Secure Email Add-In allows you to encrypt messages from your email client such as Outlook[2, p. 6-7].
B. This feature allows users to send up to 100MB of attachments in a secure email, not 50MB[2, p. 9].
D. Large file attachments can be sent using both the websafe portal and the Cisco Secure Email Add-In. The websafe portal allows you to compose and send encrypted messages from any web browser, while the Cisco Secure Email Add-In allows you to encrypt messages from your email client such as Outlook[2, p. 6-7].

QUESTION 87
Which cloud service provides a reputation verdict for email messages based on the sender domain and other attributes?

A. Cisco AppDynamics
B. Cisco Secure Email Threat Defense
C. Cisco Secure Cloud Analytics
D. Cisco Talos

Correct Answer: D
Section:
Explanation:
Cisco Talos is a cloud service that provides a reputation verdict for email messages based on the sender domain and other attributes such as IP address, sender behavior, message content, and attachment analysis. Cisco Talos is integrated with Cisco Secure Email Gateway and provides realtime threat intelligence and protection against spam, phishing, malware, and other email-borne threats.
The other options are not valid because:
A. Cisco AppDynamics is a cloud service that provides application performance monitoring and optimization for enterprise applications. It does not provide reputation verdicts for email messages.
B. Cisco Secure Email Threat Defense is a cloud service that provides visibility and remediation capabilities for email threats detected by Cisco Secure Email Gateway. It does not provide reputation verdicts for email messages.
C. Cisco Secure Cloud Analytics is a cloud service that provides network visibility and threat detection for cloud environments. It does not provide reputation verdicts for email messages.

QUESTION 88
Which type of DNS record would contain the following line, which references the DKIM public key per RFC 6376?v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A2362BECE40658267045694 3283BE

A. CNAME
B. AAAA
C. TXT
D. PTR

Correct Answer: C
Section:
Explanation:
A TXT record is a type of DNS record that contains arbitrary text data that can be used for various purposes such as verification, configuration, or authentication. A TXT record can contain the DKIM public key per RFC 6376, which is used to verify the digital signature of an email message generated by the DKIM private key of the sender domain.
The other options are not valid because:
A. A CNAME record is a type of DNS record that maps an alias name to a canonical name or another alias name. It does not contain any DKIM public key information.

B. An AAAA record is a type of DNS record that maps a hostname to an IPv6 address. It does not contain any DKIM public key information.
D. A PTR record is a type of DNS record that maps an IP address to a hostname, which is the reverse of an A or AAAA record. It does not contain any DKIM public key information.

QUESTION 89

A Cisco Secure Email Gateway administrator recently enabled the Outbreak Filters Global Service
Setting to detect Viral as well as Non-Viral threat detection, with no detection of Non-viral threats after 24 hours of monitoring Outbreak Filters What is the reason that Non-Viral threat detection is not detecting any positive verdicts?

A. Non-Viral threat detection requires Antivirus or AMP enablement to properly function
B. The Outbreak Filters option Graymail Header must be enabled
C. Non-Viral threat detection requires AntiSpam or Intelligent Multi-Scan enablement to properly function.
D. The Outbreak Filters option URL Rewriting must be enabled.

Correct Answer: C
Section:
Explanation:
According to the [Cisco Secure Email User Guide], Non-Viral threat detection is a feature of Outbreak Filters that detects and blocks email messages that contain non-viral threats such as phishing, fraud, or social engineering[1, p. 25]. To use this feature, you need to enable either AntiSpam or Intelligent Multi-Scan on your Cisco Secure Email Gateway, as these features provide the necessary scanning and filtering capabilities for Non-Viral threat detection[1, p. 26].
The other options are not valid because:
A. Non-Viral threat detection does not require Antivirus or AMP enablement to properly function.
Antivirus and AMP are features that detect and block email messages that contain viral threats such as malware or ransomware[1, p. 27-28].
B. The Outbreak Filters option Graymail Header does not affect Non-Viral threat detection. Graymail Header is an option that allows you to add a header to email messages that are classified as graymail, which are messages that are not spam but may be unwanted by some recipients, such as newsletters or promotions[1, p. 25].
D. The Outbreak Filters option URL Rewriting does not affect Non-Viral threat detection. URL Rewriting is an option that allows you to rewrite the URLs in email messages to point to a Cisco proxy server, which can scan the URLs for malicious content and redirect the users to a warning page if needed[1, p. 25].

QUESTION 90

The company security policy requires that the finance department have an easy way to apply encryption to their outbound messages that contain sensitive data Users must be able to flag the messages that require encryption versus a Cisco Secure Email Gateway appliance scanning all messages and automatically encrypting via detection Which action enables this capability?

A. Create an encryption profile with [SECURE] in the Subject setting and enable encryption on the mail flow policy
B. Create an outgoing content filter with no conditions and with the Encrypt and Deliver Now action configured with [SECURE] in the Subject setting
C. Create an encryption profile and an outgoing content filter that includes \[SECURE\] within the Subject Header: Contains condition along with the Encrypt and Deliver Now action
D. Create a DLP policy manager message action with encryption enabled and apply it to active DLP policies for outgoing mail.

Correct Answer: C
Section:
Explanation:
According to the [Cisco Secure Email Encryption Service Add-In User Guide], you can create an encryption profile that defines the encryption settings and options for your encrypted messages[2, p. 11]. You can also create an outgoing content filter that applies the encryption profile to the messages that match certain conditions, such as having [SECURE] in the subject header[2, p. 12]. This way, you can allow users to flag the messages that require encryption by adding [SECURE] to the subject line.
The other options are not valid because:
A. Creating an encryption profile with [SECURE] in the Subject setting and enabling encryption on the mail flow policy will not work, as the Subject setting in the encryption profile is used to specify the subject line of the encrypted message envelope, not the original message[2, p. 11].
B. Creating an outgoing content filter with no conditions and with the Encrypt and Deliver Now action configured with [SECURE] in the Subject setting will not work, as this will encrypt all outgoing messages regardless of whether they have [SECURE] in the subject line or not[2, p. 12].
D. Creating a DLP policy manager message action with encryption enabled and applying it to active DLP policies for outgoing mail will not work, as this will encrypt messages based on DLP rules that detect sensitive data in the message content, not based on user flags in the subject line.

QUESTION 91
An engineer wants to utilize a digital signature in outgoing emails to validate to others that the email they are receiving was indeed sent and authorized by the owner of that domain Which two components should be configured on the Cisco Secure Email Gateway appliance to achieve this?
(Choose two.)

A. DMARC verification profile
B. SPF record
C. Public/Private keypair
D. Domain signing profile
E. PKI certificate

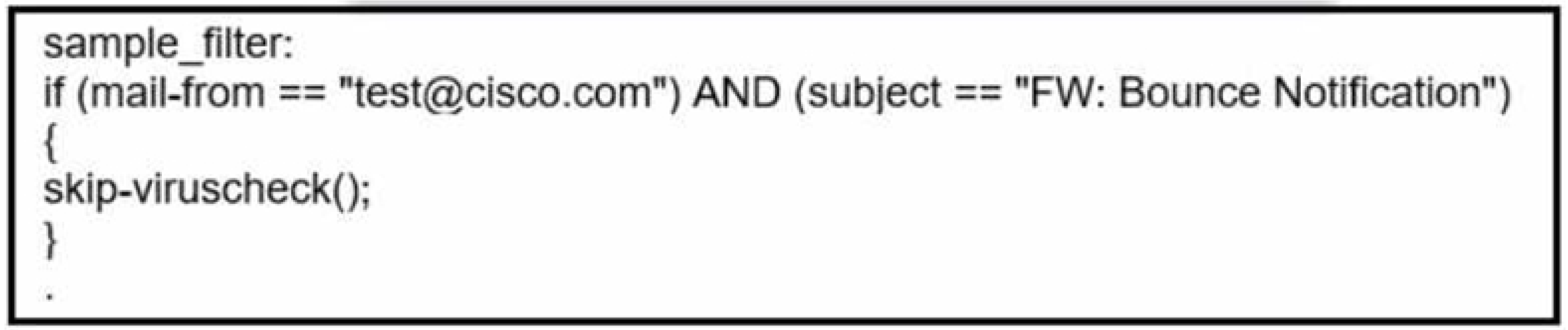
Correct Answer: C, D
Section:
Explanation:
Public/Private keypair. A public/private keypair is a pair of cryptographic keys that are used to generate and verify digital signatures. The private key is used to sign the email message, while the public key is used to verify the signature. The public key is published in a DNS record, while the private key is stored on the Cisco Secure Email Gateway appliance[1, p. 2].
Domain signing profile. A domain signing profile is a configuration that specifies the domain and selector to use for signing outgoing messages, as well as the signing algorithm, canonicalization method, and header fields to include in the signature. You can create multiple domain signing profiles for different domains or subdomains[1, p. 3].
The other options are not valid because:
A. DMARC verification profile is not a component for utilizing a digital signature in outgoing emails. It is a component for verifying the authenticity of incoming emails based on SPF and DKIM results[2, p. 1].
B. SPF record is not a component for utilizing a digital signature in outgoing emails. It is a component for validating the sender IP address of incoming emails based on a list of authorized IP addresses published in a DNS record[3, p. 1].
E. PKI certificate is not a component for utilizing a digital signature in outgoing emails. It is a component for encrypting and decrypting email messages based on a certificate authority that issues and validates certificates[4, p. 1].

QUESTION 92
What is a category for classifying graymail?

A. Malicious
B. Marketing
C. Spam
D. Priority

Correct Answer: B
Section:
Explanation:
According to the [Cisco Secure Email User Guide], graymail is a category of email messages that are not spam but may be unwanted by some recipients, such as newsletters, promotions, or social media updates[5, p. 25].
Marketing is one of the subcategories of graymail that includes messages that advertise products or services[5, p. 26].
The other options are not valid because:
A. Malicious is not a category for classifying graymail. It is a category for classifying email messages that contain malicious content such as malware, phishing, or fraud[5, p. 25].
C. Spam is not a category for classifying graymail. It is a category for classifying email messages that are unsolicited, unwanted, or harmful[5, p. 25].
D. Priority is not a category for classifying graymail. It is a category for classifying email messages that are important, urgent, or relevant[5, p. 25].

QUESTION 93
Refer to the exhibit.



```
sample_filter:
if (mail-from == "test@cisco.com") AND (subject == "FW: Bounce Notification")
{
skip-viruscheck();
}
.
```

What results from this filter configuration?

A. Action is skipping all antivirus checks for the mail

B. Action is applied to all mail that has the subject "FW: Bounce Notification."

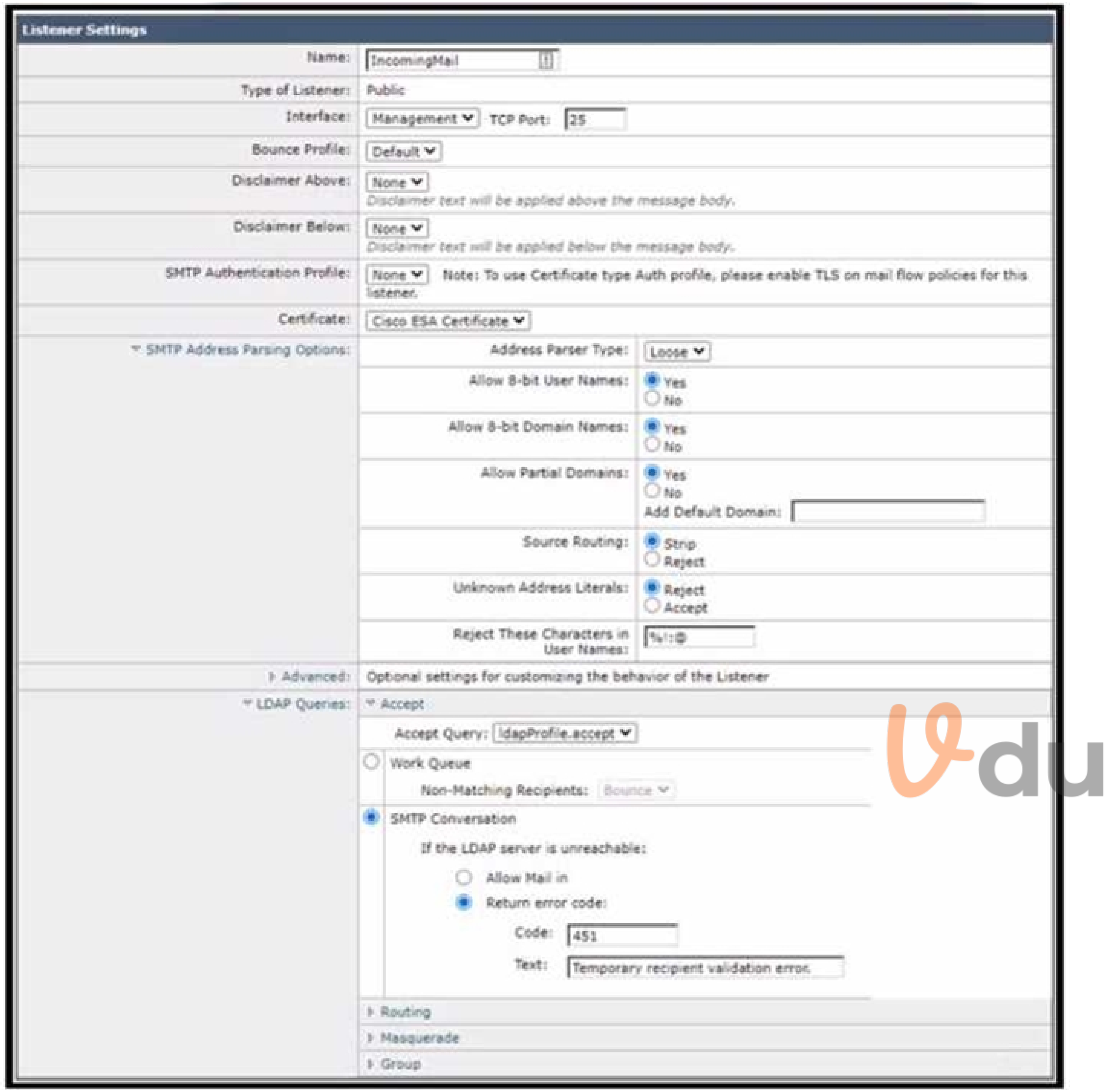
C. Action is applied to all mail from test@cisco.com.

D. Action is skipping all antispam checks for the mail.

Correct Answer: A
Section:

QUESTION 94

Refer to the exhibit.



Listener Settings

Name:	IncomingMail
Type of Listener:	Public
Interface:	Management TCP Port: 25
Bounce Profile:	Default
Disclaimer Above:	None *Disclaimer text will be applied above the message body.*
Disclaimer Below:	None *Disclaimer text will be applied below the message body.*
SMTP Authentication Profile:	None Note: To use Certificate type Auth profile, please enable TLS on mail flow policies for this listener.
Certificate:	Cisco ESA Certificate
▾ SMTP Address Parsing Options:	Address Parser Type: Loose Allow 8-bit User Names: ● Yes ○ No Allow 8-bit Domain Names: ● Yes ○ No Allow Partial Domains: ● Yes ○ No Add Default Domain: Source Routing: ● Strip ○ Reject Unknown Address Literals: ● Reject ○ Accept Reject These Characters in User Names: %!:@
▸ Advanced:	Optional settings for customizing the behavior of the Listener
▾ LDAP Queries:	▾ Accept Accept Query: ldapProfile.accept ○ Work Queue Non-Matching Recipients: Bounce ● SMTP Conversation If the LDAP server is unreachable: ○ Allow Mail in ● Return error code: Code: 451 Text: Temporary recipient validation error. ▸ Routing ▸ Masquerade ▸ Group

Which additional configuration action must be taken to protect against Directory Harvest Attacks?

A. When LDAP Queries are configured, Directory Harvest Attack Prevention is enabled by default.

B. In the LDAP Server profile, configure Directory Harvest Attack Prevention

C. In the mail flow policy, configure Directory Harvest Attack Prevention.

D. In the Listener Settings, modify the LDAP Queries configuration to use the Work Queue

Correct Answer: C
Section:
Explanation:
To protect against Directory Harvest Attacks, the administrator must configure Directory Harvest Attack Prevention in the mail flow policy that applies to the listener. This will enable the Cisco Secure Email Gateway to reject or throttle messages that are sent to invalid recipients by checking the LDAP server for valid email addresses. Reference: [Cisco Secure Email Gateway Administrator Guide -Configuring Directory

Harvest Attack Prevention]

QUESTION 95

An organization has multiple Cisco Secure Email Gateway appliances deployed, resulting in several spam quarantines to manage. To manage the quarantined messages, the administrator enabled the centralized spam quarantine on the Cisco Secure Email and Web Manager appliance and configured the external spam quarantine on the Cisco Secure Email Gateway appliances. However, messages are still being directed to the local quarantine on the Cisco Secure Email Gateway appliances What change is necessary to complete the configuration?

A. Modify the incoming mail policies on the Cisco Secure Email Gateway appliances to redirect to the external quarantine
B. Disable the external spam quarantine on the Cisco Secure Email Gateway appliances
C. Disable the local spam quarantine on the Cisco Secure Email Gateway appliances.
D. Modify the external spam quarantine settings on the Cisco Secure Email Gateway appliances and change the port to 25

Correct Answer: C
Section:
Explanation:
To use the centralized spam quarantine on the Cisco Secure Email and Web Manager appliance, the administrator must disable the local spam quarantine on the Cisco Secure Email Gateway appliances.
This will prevent messages from being stored in both quarantines and avoid confusion for end users and administrators. Reference: [Cisco Secure Email and Web Manager User Guide - Configuring Centralized Spam Quarantine]

QUESTION 96

An organization has a strict policy on URLs embedded in emails. The policy allows visibility into what the URL is but does not allow the user to click it. Which action must be taken to meet the requirements of the security policy?

A. Enable the URL quarantine policy
B. Defang the URL.
C. Replace the URL with text
D. Redirect the URL to the Cisco security proxy

Correct Answer: B
Section:
Explanation:
To meet the security policy of allowing visibility into what the URL is but not allowing the user to click it, the administrator must defang the URL. This means that the URL will be modified in a way that it is still readable by humans but not clickable by browsers. For example, http://example.com could be defanged as hxxp://example[.]com. Reference: [Cisco Secure Email Gateway Administrator Guide -Defanging URLs in Messages]

QUESTION 97

Which components are required when encrypting SMTP with TLS on a Cisco Secure Email Gateway appliance when the sender requires TLS verification?

A. DER certificate and matching public key from a CA
B. self-signed certificate in PKCS#7 format
C. X. 509 certificate and matching private key from a CA
D. self-signed certificate in PKCS#12 format

Correct Answer: C
Section:
Explanation:
To encrypt SMTP with TLS on a Cisco Secure Email Gateway appliance when the sender requires TLS verification, the components that are required are an X.509 certificate and matching private key from a CA. The certificate must be signed by a trusted CA and contain the domain name or IP address of the listener in the Subject or Subject Alternative Name fields. The private key must be unencrypted and match the certificate. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring TLS]

QUESTION 98

Which content filter condition checks to see if the "From: header" in the message is similar to any of the users in the content dictionary?

A. Forged Email Detection
B. SPF Verification
C. Subject Header
D. Duplicate Boundaries Verification

Correct Answer: A
Section:
Explanation:

The content filter condition that checks to see if the "From: header" in the message is similar to any of the users in the content dictionary is Forged Email Detection. This condition compares the sender's name or email address with a list of names or email addresses in a content dictionary and triggers an action if they match or are similar. Reference: [Cisco Secure Email Gateway Administrator Guide - Forged Email Detection]

QUESTION 99

An engineer must provide differentiated email filtering to executives within the organization Which two actions must be taken to accomplish this task? (Choose two)

A. Define an LDAP group query to specify users to whom the mail policy rules apply.
B. Create content filters for actions to take on messages that contain specific data
C. Upload a csv file containing the email addresses for the users for whom you want to create mail policies.
D. Enable the content-scanning features you want to use with mail policies
E. Define the default mail policies for incoming or outgoing messages

Correct Answer: A, B
Section:
Explanation:

Define an LDAP group query to specify users to whom the mail policy rules apply. This way, you can create a custom group of executive users and apply different mail policies to them based on their LDAP attributes[4, p. 2].
Create content filters for actions to take on messages that contain specific data. Content filters allow you to scan the message body and attachments for keywords, phrases, or patterns that match your criteria and perform actions such as quarantine, encrypt, or drop the message[4, p. 7].
The other options are not valid because:
C. Uploading a csv file containing the email addresses for the users for whom you want to create mail policies is not a supported feature of Cisco Secure Email1.
D. Enabling the content-scanning features you want to use with mail policies is not necessary, as content scanning is enabled by default for all incoming and outgoing messages[4, p. 6].
E. Defining the default mail policies for incoming or outgoing messages is not sufficient, as default mail policies apply to all users and do not allow for differentiation based on user groups[4, p. 2].

QUESTION 100

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. Enable the Forged Email Detection feature under Security Settings.
C. Enable DMARC feature under Mail Policies.
D. Create an incoming content filter with the Forged Email Detection condition
E. Create a content dictionary including a list of the names that are being spoofed.

Correct Answer: D, E
Section:
Explanation:

To ensure that executive messages are originating from legitimate sending addresses, the administrator must take two steps:

Create an incoming content filter with the Forged Email Detection condition. This will allow the administrator to detect and block messages that have a forged "From: header" that matches or is similar to any of the names in a content dictionary.

Create a content dictionary including a list of the names that are being spoofed. This will allow the administrator to specify the names of the executives that are being targeted by spoofing attacks and use them in the Forged Email Detection condition. The other options are not relevant or sufficient for this task. Reference: [Cisco Secure Email Gateway Administrator Guide - Forged Email Detection] and [Cisco Secure Email Gateway Administrator Guide - Creating Content Dictionaries]