ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which SMTP extension does Cisco ESA support for email security?

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

Answer: D

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: 2

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

Answer: A

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: 3

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

Answer: C

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: 4

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

Answer: D

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: 5

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

Answer: BE

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: 6

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

A. reject
B. workqueue
C. action
D. delivery
E. quarantine

Answer: BD

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: 7

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

Answer: AD

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: 8

Which setting affects the aggressiveness of spam detection?

A. protection level

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

Answer: B

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: 9

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.

Answer: D

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: 10

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

Answer: D

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: 11

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.

Answer: AC

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: 12

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.

Associate the filter with a nominated incoming mail policy.

Configure a filter to take necessary action on SPF/SIDF verification results.

Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.

Test the results of message verification.

Configure a sendergroup to use the custom mail-flow policy.

step 1

step 2

step 3

step 4

step 5

Answer:

Explanation:

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.

Question: 13

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

Answer: A

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: 14

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.

Answer: D

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: 15

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.

Add a new fitter 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

Answer:

Explanation:

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.

Reference:

https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/td- p/2441383

Question: 16

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

Answer: B

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: 17

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

Answer: B

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: 18

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

Answer: D

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: 19

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

Answer: BE

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: 20

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

Answer: B

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: 21

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.

Answer: A

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: 22

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

Answer: BD

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: 23

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.

Answer: BE

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: 24

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

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

Answer: B

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

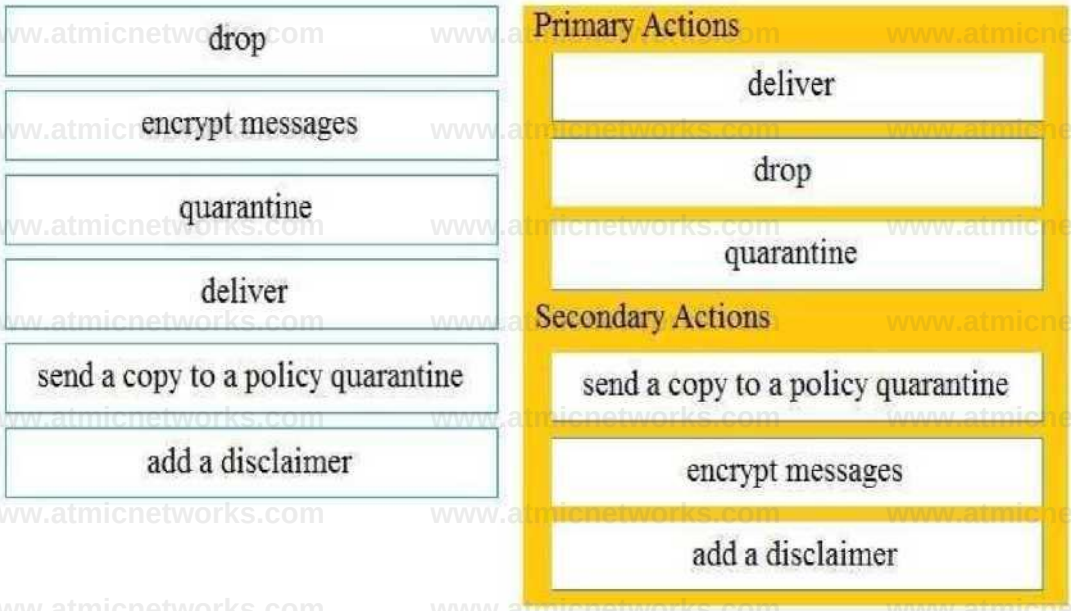
Question: 25

DRAG DROP

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

Answer:

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: 26

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

Answer: AD

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: 27

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.

Answer: AD

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: 28

What occurs when configuring separate incoming mail policies?

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

Answer: A

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: 29

Which type of query must be configured when setting up the Spam Quarantine while merging notifications?

A. Spam Quarantine Alias Routing Query
B. Spam Quarantine Alias Consolidation Query
C. Spam Quarantine Alias Authentication Query
D. Spam Quarantine Alias Masquerading Query

Answer: B

Explanation:

Spam Quarantine Alias Consolidation Query is a type of query that must be configured when setting up the Spam Quarantine while merging notifications on Cisco ESA. This query allows Cisco ESA to consolidate multiple email addresses that belong to the same end user into one entry in the Spam Quarantine, and send only one notification email to that end user with all the quarantined messages for all their email addresses.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-10.

Question: 30

Which two factors must be considered when message filter processing is configured? (Choose two.)

A. message-filter order
B. lateral processing
C. structure of the combined packet
D. mail policies
E. MIME structure of the message

Answer: AE

Explanation:

Message-filter order and MIME structure of the message are two factors that must be considered when message filter processing is configured on Cisco ESA. Message-filter order determines the sequence in which message filters are evaluated and applied to incoming messages, which can affect the final outcome of the filtering process. MIME structure of the message determines how message filters match against different parts of the message, such as headers, body, attachments, etc., which can affect the accuracy and performance of the filtering process.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 3-3 and page 3-5.

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_chapter_01000.html

Question: 31

How does the graymail safe unsubscribe feature function?

A. It strips the malicious content of the URI before unsubscribing.
B. It checks the URI reputation and category and allows the content filter to take an action on it.
C. It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.
D. It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.

Answer: D

Explanation:

Secure unsubscribe option for end users. Mimicking an unsubscribe option is a popular phishing technique. For this reason, the end users are generally wary of clicking unknown unsubscribe links. For such scenarios, the cloud-based Unsubscribe Service extracts the original unsubscribe URI, checks the reputation of the URI, and then performs the unsubscribe process on behalf of the end user. This protects end users from malicious threats masquerading as unsubscribe links.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2- 1/User_Guide/b_ESA_Admin_Guide_14-2-1/b_ESA_Admin_Guide_12_1_chapter_01110.html#id_101033

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

Question: 32

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.

Answer: B

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: 33

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.

Answer: D

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-technote- esa-00.html
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026- technote- esa-00.html

Question: 34

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

Answer: B

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 AntiVirus 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: 35

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

Answer: B

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: 36

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

Answer: C

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: 37

Which attack is mitigated by using Bounce Verification?

A. spoof
B. denial of service
C. eavesdropping
D. smurf

Answer: B

Explanation:

Bounce Verification is a feature that mitigates denial of service attacks on Cisco ESA. A denial of service attack is an attempt to overwhelm a system or network with excessive traffic or requests, rendering it unavailable or slow for legitimate users. Bounce Verification prevents Cisco ESA from accepting bounce messages that are not generated by itself or by trusted hosts, reducing the load on

the system and preventing backscatter spam.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 5-8.

Reference: https://www.networkworld.com/article/2305394/ironport-adds-bounce-back-verification-for-e- mail.html

Question: 38

When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)

A. redirect
B. return
C. drop
D. delay
E. abandon

Answer: AD

Explanation:

The Outbreak Filters feature uses three tactics to protect your users from outbreaks: Delay.
Redirect.
Modify.

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: 39

Which two features are applied to either incoming or outgoing mail policies? (Choose two.)

A. Indication of Compromise
B. application filtering
C. outbreak filters
D. sender reputation filtering
E. antivirus

Answer: CE

Explanation:

Outbreak filters and antivirus are two features that can be applied to either incoming or outgoing mail policies on Cisco ESA. Outbreak filters allow Cisco ESA to detect and block messages that contain new or emerging email threats, such as viruses, worms, phishing, or spam, by using real-time updates from Talos intelligence. Antivirus allows Cisco ESA to scan messages for known viruses and malware using one or two antivirus engines (Sophos and McAfee).
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 6-16 and page 7-2.

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_01001.html

Question: 40

What must be configured to allow the Cisco ESA to encrypt an email using the Cisco Registered Envelope Service?

A. provisioned email encryption profile
B. message encryption from a content filter that select "Message Encryption" over TLS
C. message encryption from the mail flow policies with "CRES" selected
D. content filter to forward the email to the Cisco Registered Envelope server

Answer: A

Explanation:

To allow the Cisco ESA to encrypt an email using the CRES (Cisco Registered Envelope Service), a provisioned email encryption profile must be configured on Cisco ESA. A provisioned email encryption profile is a type of encryption profile that specifies how messages are encrypted using CRES, such as the encryption key strength, the notification options, the branding settings, etc.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 12-4.

Question: 41

Which two configurations are used on multiple LDAP servers to connect with Cisco ESA? (Choose two.)

A. load balancing
B. SLA monitor
C. active-standby
D. failover
E. active-active

Answer: AD

Explanation:

Load balancing and failover are two configurations that can be used on multiple LDAP servers to connect with Cisco ESA. Load balancing means that Cisco ESA will distribute the LDAP queries among the available LDAP servers in a round-robin fashion, improving the performance and efficiency of the LDAP queries. Failover means that Cisco ESA will switch to another LDAP server if the current one is unavailable or unresponsive, ensuring the continuity and reliability of the LDAP queries.

Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-8.

You can enter multiple host names to configure the LDAP servers for failover or load-balancing.
Separate multiple entries with commas.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/sma_user_guide/b_SMA_Admin_Guide_ces_11/b_SMA_Admin_Guide_chapter_01010.html

Question: 42

What is the default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine?

A. 8025
B. 6443
C. 6025
D. 8443

Answer: C

Explanation:

The default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine is 6025. This is the default value for the Port setting in the External Spam Quarantine configuration on Cisco ESA. This port must be open on both Cisco ESA and Cisco SMA for the communication to work.

Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-4.

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692- configure- esa-00.html

Question: 43

DRAG DROP

Drag and drop the AsyncOS methods for performing DMARC verification from the left into the correct order on the right.

AsyncOS performs DMARC verification on the message.	step 1
A Listener configured on AsyncOS receives an SMTP connection.	**step 2**
AsyncOS performs SPF and DKTM verification on the message.	**step 3**
AsyncOS fetches the DMARC record for the sender domain from the DNS.	step 4

Answer:

Explanation:

AsyncOS performs DMARC verification on the message.	A listener configured on AsyncOS receives an SMTP connection.
A listener configured on Async OS receives an SMTP connection.	AsyncOS performs SPF and DKIM verification on the message.
AsyncOS performs SPF and DKIM verification on the message.	AsyncOS fetches the DMARC record for the sender domain from the DNS.
AsyncOS fetches the DMARC record for the sender domain from the DNS.	AsyncOS performs DMARC verification on the message.

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_010101.html

Question: 44

Which two steps are needed to disable local spam quarantine before external quarantine is enabled? (Choose two.)

A. Uncheck the Enable Spam Quarantine check box.
B. Select Monitor and click Spam Quarantine.
C. Check the External Safelist/Blocklist check box.
D. Select External Spam Quarantine and click on Configure.
E. Select Security Services and click Spam Quarantine.

Answer: AE

Explanation:

To disable local spam quarantine before external quarantine is enabled on Cisco ESA, two steps are needed:
Select Security Services and click Spam Quarantine, which will open the Spam Quarantine settings page.
Uncheck the Enable Spam Quarantine check box, which will disable the local spam quarantine feature on Cisco ESA.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 10-2.

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa- 00.html (configuration summary)

Question: 45

Which Cisco ESA security service is configured only through an outgoing mail policy?

A. antivirus
B. DLP
C. Outbreak Filters
D. AMP

Answer: B

Explanation:

DLP (Data Loss Prevention) is a security service that is configured only through an outgoing mail policy on Cisco ESA. DLP allows Cisco ESA to scan outgoing messages for sensitive or confidential data, such as credit card numbers, social security numbers, health records, etc., and apply appropriate actions, such as encrypt, quarantine, notify, etc., to prevent data leakage or loss.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2.

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_01001.html

Question: 46

Which two components must be configured to perform DLP scanning? (Choose two.)

A. Add a DLP policy on the Incoming Mail Policy.
B. Add a DLP policy to the DLP Policy Manager.

C. Enable a DLP policy on the Outgoing Mail Policy.
D. Enable a DLP policy on the DLP Policy Customizations.
E. Add a DLP policy to the Outgoing Content Filter.

Answer: BC

Explanation:

To perform DLP scanning on Cisco ESA, two components must be configured:
Add a DLP policy to the DLP Policy Manager, which is a repository of predefined or custom DLP policies that specify what types of data to scan for and what actions to take if a match is found.
Enable a DLP policy on the Outgoing Mail Policy, which is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2 and page 9-4.

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_010001.html

Question: 47

Which two certificate authority lists are available in Cisco ESA? (Choose two.)

A. default
B. system
C. user
D. custom
E. demo

Answer: BD

Explanation:

System: This is the default list of trusted certificate authorities that is provided by Cisco and updated automatically. It contains the certificates of well-known and widely used certificate authorities, such as VeriSign, Thawte, and GoDaddy.
Custom: This is the list of additional certificate authorities that you can add manually or import from a file. It allows you to trust certificates that are issued by your own or third-party certificate authorities that are not included in the system list.

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_011000.html#task_1194859

Question: 48

Which two are configured in the DMARC verification profile? (Choose two.)

A. name of the verification profile
B. minimum number of signatures to verify
C. ESA listeners to use the verification profile
D. message action into an incoming or outgoing content filter
E. message action to take when the policy is reject/quarantine

Answer: AE

Explanation:

A DMARC verification profile is a list of parameters that the mail flow policies of the appliance use for verifying DMARC. The name of the verification profile identifies the profile and allows you to apply it to different mail flow policies. The message action to take when the policy is reject/quarantine determines how the appliance handles messages that fail DMARC verification based on the sender's DMARC policy.

Reference: User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment), Chapter: Email Authentication, Section: Configuring DMARC Verification

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_010101.html#task_1231917

Question: 49

Which two components form the graymail management solution in Cisco ESA? (Choose two.)

A. cloud-based unsubscribe service
B. uniform unsubscription management interface for end users
C. secure subscribe option for end users
D. integrated graymail scanning engine
E. improved mail efficacy

Answer: AD

Explanation:

The graymail management solution in the appliance comprises of two components: an integrated graymail scanning engine and a cloud-based Unsubscribe Service. The integrated graymail scanning engine identifies graymail messages using various criteria and assigns them to different categories. The cloud-based Unsubscribe Service provides an easy mechanism for end users to unsubscribe from unwanted messages by checking the reputation of the unsubscribe links and performing the unsubscribe process on behalf of the end user.

Reference: User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment), Chapter: Managing Graymail, Section: Graymail Management Solution in Email Security Appliance

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_01101.pdf (p.2)

Question: 50

When URL logging is configured on a Cisco ESA, which feature must be enabled first?

A. antivirus
B. antispam
C. virus outbreak filter
D. senderbase reputation filter

Answer: C

Explanation:

Enabling Logging of URLs and Message Tracking Details for URLs
Logging of URL-related logs, and display of this information in Message Tracking details, is disabled by default. This includes the logs for the following events:

Category of any URL in the message matches the URL category filters
Reputation score of any URL in the message matches URL reputation filters
Outbreak Filter rewrites any URL in the message
To enable logging of these events, use the outbreakconfig command in the command-line interface (CLI).

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_01110.html?bookSearch=t rue
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote- esa-00.html (note under enable url filtering)

Question: 51

What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

A. 83
B. 82
C. 443
D. 80

Answer: A

Explanation:

in the spam quarantine section, you can configure settings for access to the spam quarantine, and by default, HTTP uses port 82 and HTTPS uses port 83.

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_011111.pdf

Question: 52

What is a benefit of implementing URL filtering on the Cisco ESA?

A. removes threats from malicious URLs
B. blacklists spam
C. provides URL reputation protection
D. enhances reputation against malicious URLs

Answer: C

Explanation:

A benefit of implementing URL filtering on the ESA is that it provides URL reputation protection. URL filtering uses SenderBase, a web-based service that collects information about URLs and domains from various sources, to assign a reputation score and a category to each URL. Based on these attributes, you can configure content or message filters to take actions on messages containing malicious or

undesirable URLs.

Reference: User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment), Chapter: Protecting Against Malicious or Undesirable URLs, Section: URL-Related Protections and Controls

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775- technote- esa-00.html

Question: 53

Refer to the exhibit.

Which SPF record is valid for mycompany.com?

A. v=spf1 a mx ip4:199.209.31.2 -all
B. v=spf1 a mx ip4:10.1.10.23 -all
C. v=spf1 a mx ip4:199.209.31.21 -all
D. v=spf1 a mx ip4:172.16.18.230 -all

Answer: C

Explanation:

The SPF record for mycompany.com is shown in the exhibit as:

v=spf1 a mx ip4:199.209.31.21 -all

This means that the domain mycompany.com authorizes the following sources to send email on its behalf:

The A record of mycompany.com, which resolves to 199.209.31.21

The MX record of mycompany.com, which points to mail.mycompany.com, which also resolves to 199.209.31.21

The IP address 199.209.31.21

The -all qualifier means that any other source is not authorized and should be rejected.

Therefore, the correct answer is C.

Reference:

SPF Record Syntax

Define your SPF record—Basic setup

Question: 54

What is a valid content filter action?

A. decrypt on delivery

B. quarantine
C. skip antispam
D. archive

Answer: B

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: 55

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

Answer: AB

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: 56

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

Answer: C

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: 57

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

Answer: C

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-scan- behavior- impact-on-av/td-p/3923243

Question: 58

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.

Answer: C

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: 59

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.

Answer: A

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: 60

What are two primary components of content filters? (Choose two.)
A. conditions
B. subject
C. content
D. actions
E. policies

Answer: AD

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: 61

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

Answer: BD

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: 62

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

Answer: A

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: 63

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.

Answer: C

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?bookSearc h=true#con_1172419

Question: 64

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.

Answer: B

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: 65

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

Answer: A

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=t rue

Question: 66

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.

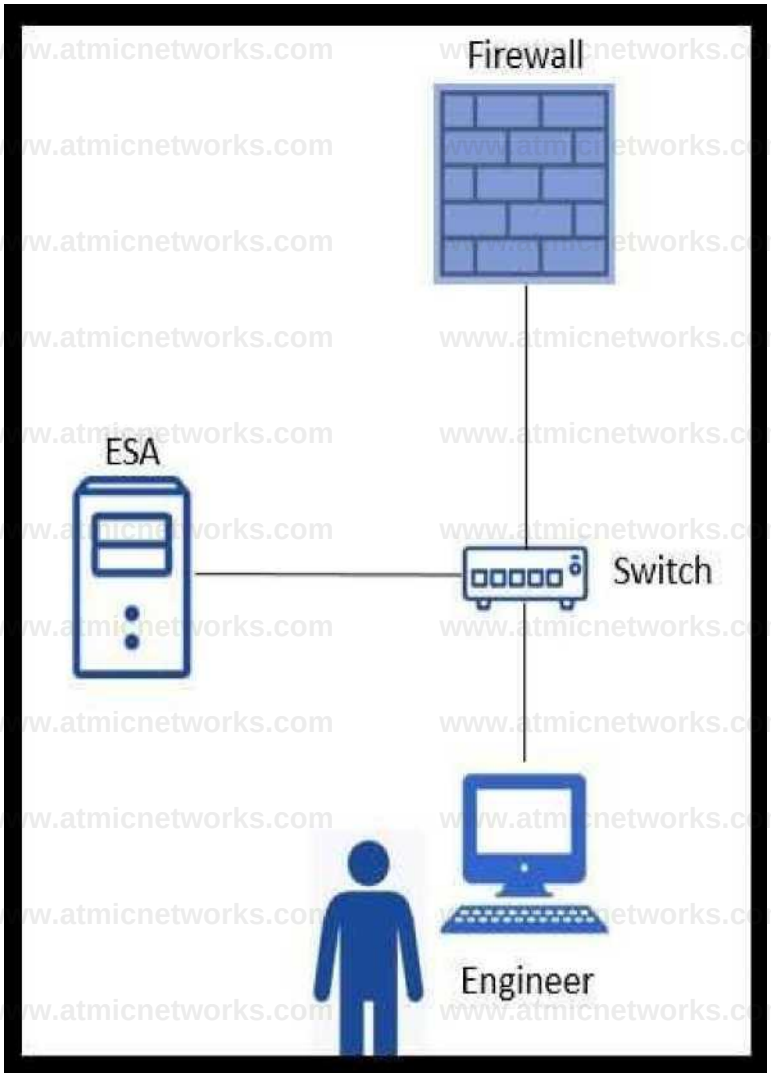
Answer: C

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: 67



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

Answer: D

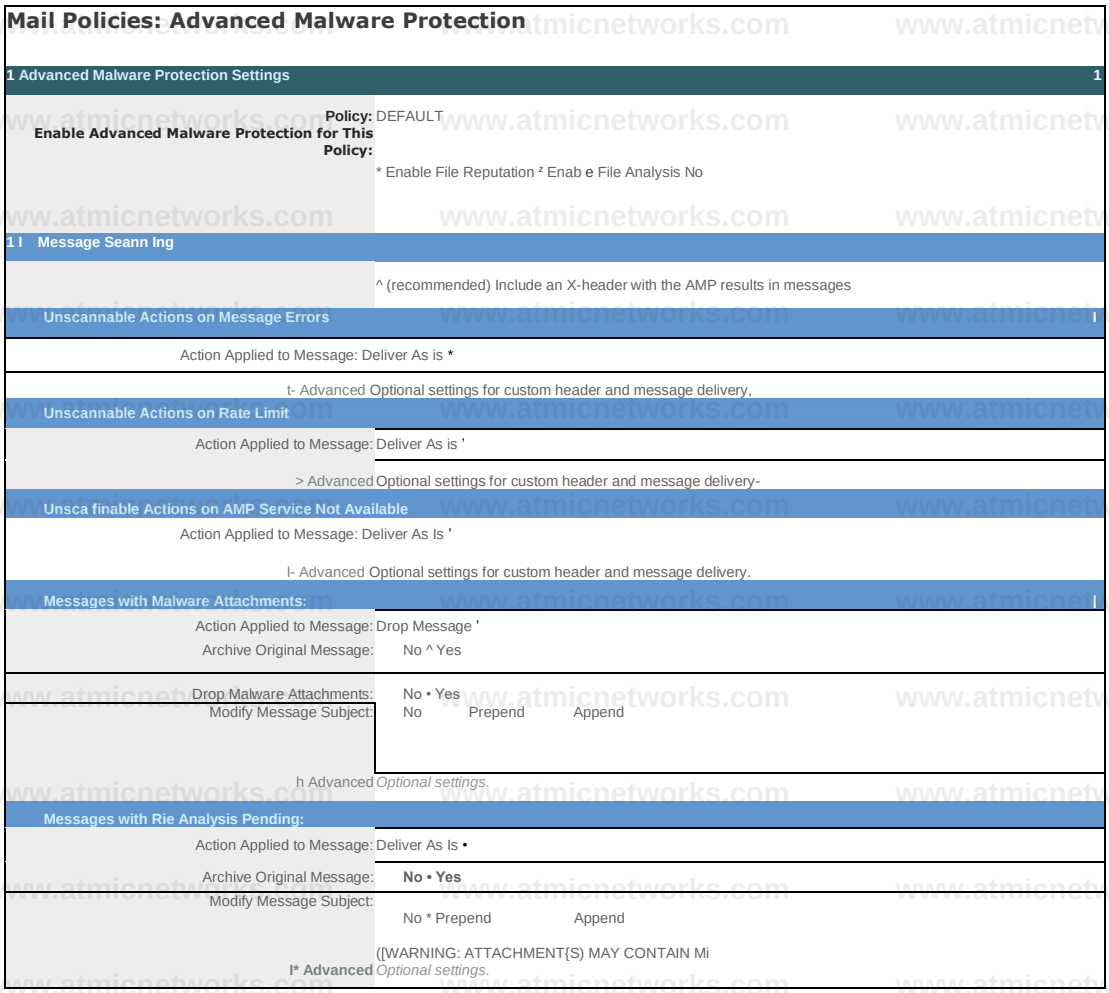
Explanation:

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: 68



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.

Answer: B

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: 69

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.

Answer: D

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: 70

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.

Answer: D

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: 71

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

Answer: BC

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: 72

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.

Answer: A

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: 73

```
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".

Answer: D

Explanation:

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKSEC-2240.pdf

Question: 74

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

Answer: D

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: 75

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

Answer: A

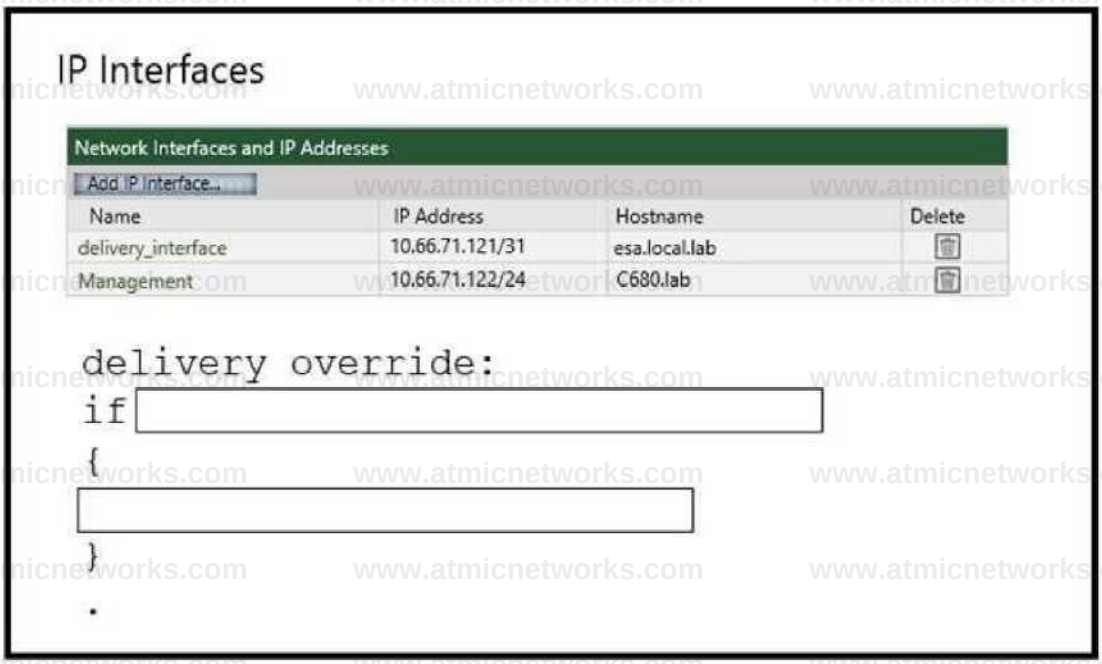
Explanation:

Outgoing Mail Policy is a mail policy that should be created to accomplish this task. Outgoing Mail Policy is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.
To create an Outgoing Mail Policy named 'Sales' and assign a DLP policy to it, the administrator can follow these steps:
Select Mail Policies > Outgoing Mail Policies and click Add Policy.
Enter 'Sales' as the policy name and click Submit.
Select 'Sales' from the list of policies and click Edit Settings.
Under Data Loss Prevention, select Enable Data Loss Prevention Scanning and choose the DLP policy from the drop-down menu.
Click Submit.
The other options are not valid mail policies to accomplish this task, because they do not apply to outgoing messages or DLP scanning.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2 and page 9-4.

Question: 76

DRAG DROP

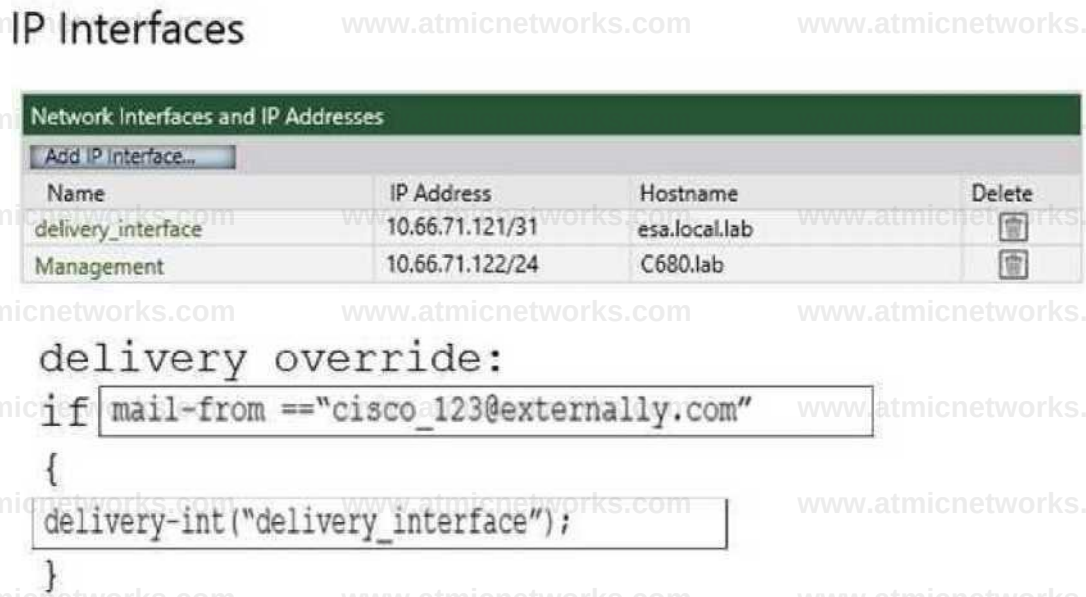
An administrator must ensure that emails sent from cisco_123@externally.com are routed through an alternate virtual gateway. Drag and drop the snippet from the bottom onto the blank in the graphic to finish the message filter syntax. Not all snippets are used.




```
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”);
```

Answer:

Explanation:



Question: 77

Spreadsheets containing credit card numbers are being allowed to bypass the Cisco ESA.

Which outgoing mail policy feature should be configured to catch this content before it leaves the network?

A. file reputation filtering
B. outbreak filtering
C. data loss prevention
D. file analysis

Answer: C

Explanation:

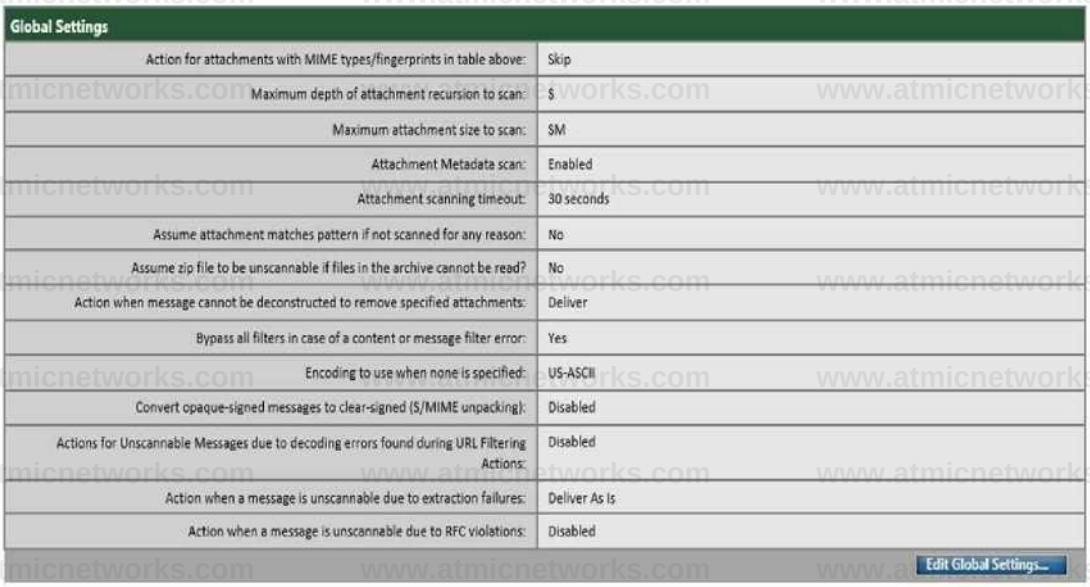
Data Loss Prevention (DLP) is an outgoing mail policy feature that should be configured to catch this content before it leaves the network. DLP allows Cisco ESA to scan outgoing messages for sensitive or confidential data, such as credit card numbers, social security numbers, health records, etc., and apply appropriate actions, such as encrypt, quarantine, notify, etc., to prevent data leakage or loss. The other options are not valid outgoing mail policy features to catch this content before it leaves the network, because they do not scan for sensitive or confidential data in messages.

Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2 and page 9-3.

Question: 78

```
Tue Aug 13 16:55:40 2019 Info: Start MID 379133 ICID 391963
Tue Aug 13 16:55:40 2019 Info: MID 379133 ICID 391963 From: <matt@lee.com>
Tue Aug 13 16:55:40 2019 Info: MID 379133 ICID 391963 AID o To: <bob_doe@cisco.com>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Message-ID '<op.z6f21uf7uxysu20mathuynh-f645d.inshDme.net>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Subject 'This is a highly confidential email.'
Tue Aug 13 16:55:48 2019 Info: MID 379133 ready 12142757 bytes from <matt@lee.com>
Tue Aug 13 16:55:49 2019 Info: MED 379133 matchedall recipients for pre-recipient policy marketing team in th* inbound table
Tue Aug 13 16:55:49 2019 Info: MED 379133 was too big (12142757/524208) for scanning by Outbreak Filters
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/2097152i for scanning by CASE
Tue Aug 13 16:55:50 2019 Info: MID 379133 interimAV verdict using Sophos CLEAN
Tue Aug 13 16:55:50 2019 Info: MID 379133 antivirus negative
Tue Aug 13 16:55:50 2019 Info: MED 379133 using engine: GRAYMAIL negative
Tue Aug 13 16:55:52 2019 Info: MID 379133 attachment 'ds_validation_NEG.zip'
Tue Aug 13 16:55:52 2019 warning: MID 379133, Message Scanning Problem: Size Limit Exceeded
Tue Aug 13 16:55:52 2019 Info: MID 379133 queued for delivery
```

Scan Behavior



Global Settings	
Action for attachments with MIME types/fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled
	Edit Global Settings...

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

A. Add an additional mapping for attachment type for zip files.
B. Enable assume match pattern if the email was not scanned for any reason.
C. Increase the maximum recursion depth from 5 to a larger value.
D. Increase the maximum attachment size to scan to a larger value.

Answer: D

Explanation:

The maximum attachment size to scan is a configuration on the scan behavior that determines the maximum size of an attachment that Cisco ESA will scan for viruses and malware. If an attachment exceeds this size, Cisco ESA will apply the configured action for unscannable messages, such as deliver, drop, or quarantine.
To allow the attachment to be scanned on the Cisco ESA, this configuration must be updated to a larger value than the attachment size, which is 10 MB according to the message header.
The other options are not valid configurations to allow the attachment to be scanned on the Cisco ESA, because they do not affect the maximum attachment size to scan.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 7-3 and page 7-4.

Question: 79

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

Answer: AE

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: 80

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

Answer: D

Explanation:

The correct order of commands to set filter 2 to active on the CLI of Cisco ESA is: filters, which enters the message filter mode.
set, which sets the status of one or more message filters.
2, which specifies the message filter number.
1, which sets the status of message filter 2 to active.
The other options are not valid orders of commands to set filter 2 to active on the CLI of Cisco ESA, because they use incorrect commands or parameters.
Reference: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page A-6 and page A-7.

Question: 81

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

Answer: A

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.

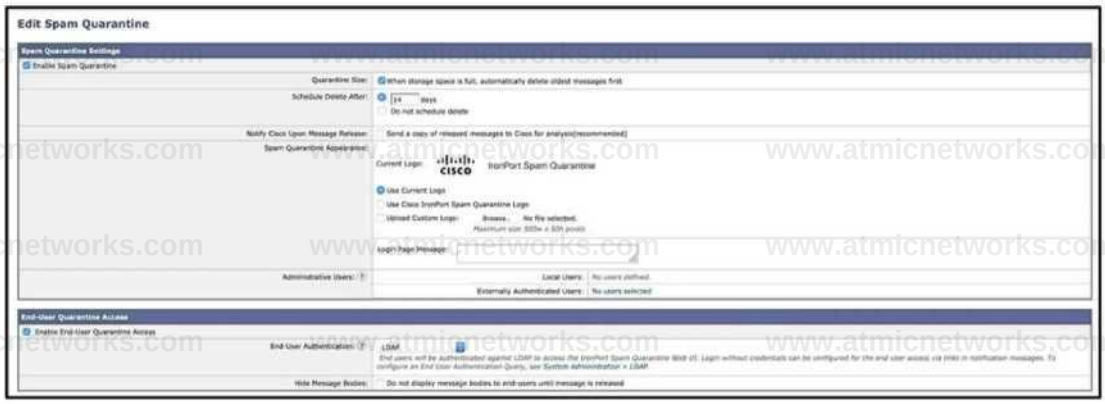
Under SMTP Authentication Settings, select Enable Directory Harvest Attack Prevention.

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: 82



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.

Answer: D

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: 83

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

Answer: B

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: 84

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.

Answer: A

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: 85

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

Answer: A

Explanation:

Question: 86

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

Answer: D

Explanation:

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

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

Select Mail Policies > Content Filters and click Add Filter.
Enter a name and description for the content filter.
Under Conditions, click Add Condition.

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

Choose Fail from the drop-down menu.

Click Submit.

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

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

Question: 87

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

Answer: AC

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: 88

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 ES
A. 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.

Answer: B

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: 89

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.

Answer: AB

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: 90

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

Answer: D

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: 91

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.

Answer: C

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: 92

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

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

Answer: C

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: 93

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

Answer: DE

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: 94

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

Answer: B

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: 95

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

Answer: B, E

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: 96

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

Answer: A

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: 97

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

Answer: B

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: 98

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

Answer: D

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: 99

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

Answer: B, C

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: 100

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.

Answer: D, E

Explanation:

Question: 101

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

Answer: C

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: 102

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

Answer: B

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: 103

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

Answer: A

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: 104

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

Answer: D

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.

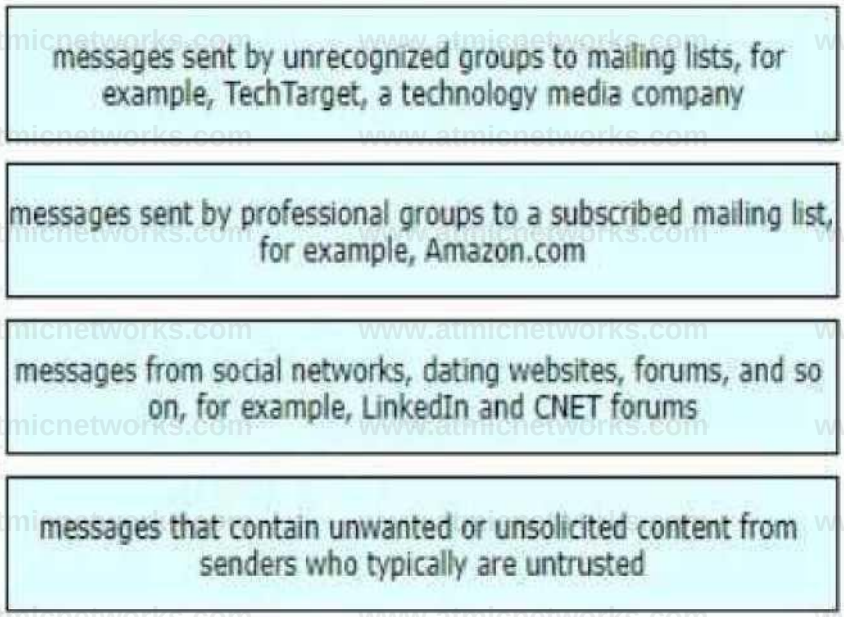
Question: 105

DRAG DROP

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

Answer:

Explanation:



Question: 106

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

Answer: D

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: 107

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

Answer: C

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: 108

An engineer deploys a Cisco Secure Email Gateway appliance with default settings in an organization that permits only standard H feature does not work. Which additional action resolves the issue?

A. Configure the outbound firewall rule to permit traffic on port 8081

B. Enable the Use HTTP option under Advanced Settings for File Reputation.

C. Enable the Use SSL option under Advanced Settings for File Reputation.

D. Configure the outbound firewall rule to permit traffic on port 3237

E. TP/HTTPS ports outbound and notices that the AMP file reputation

Answer: E

Explanation:

Configuring the outbound firewall rule to permit traffic on port 3237 is the additional action that resolves the issue. AMP file reputation is a feature that allows Cisco ESA to check files attached to messages against a cloud-based database of known malicious files and apply appropriate actions, such as block, deliver, or quarantine.
By default, AMP file reputation uses TCP port 3237 to communicate with the cloud-based database. If this port is blocked by a firewall, AMP file reputation will not work properly.
To resolve this issue, the administrator can configure the outbound firewall rule to permit traffic on port 3237 from Cisco ESA.
The other options are not valid actions to resolve the issue, because they do not affect the port used by AMP file reputation.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 7-5 and page 7-6.

Question: 109

Refer to the exhibit.

A network engineer must set up a content filter to find any messages that failed SPF and send them into quarantine The content filter has been set up and enabled, but all messages except those that have failed SPF are being sent into quarantine. Which section of the filter must be modified to correct this behavior?

A. skip-filters
B. log-entry
C. spf-status
D. quarantine

Answer: C

Explanation:

spf-status is the section of the filter that must be modified to correct this behavior. spf-status is a condition that determines whether a message matches the content filter rule based on the result of SPF verification, such as pass, fail, neutral, etc.
The content filter in the exhibit has a spf-status condition set to “Pass”, which means that it will match messages that passed SPF verification and apply the action of “Quarantine”. This is the opposite of what the network engineer intended to do.
To correct this behavior, the network engineer can modify the spf-status condition to “Fail”, which means that it will match messages that failed SPF verification and apply the action of “Quarantine”. The other options are not valid sections of the filter that must be modified to correct this behavior, because they do not affect the spf-status condition.
Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 8-3 and page 8-4.

Question: 110

Which restriction is in place for end users accessing the spam quarantine on Cisco Secure Email Gateway appliances?

A. Access via a link in a notification is mandatory.
B. The end user must be assigned to the Guest role
C. Direct access via web browser requires authentication.
D. Authentication is required when accessing via a link in a notification.

Answer: C

Explanation:

Direct access via web browser requires authentication is the restriction that is in place for end users accessing the spam quarantine on Cisco Secure Email Gateway appliances. Spam quarantine is a feature that allows Cisco ESA to store messages that are suspected to be spam and allow end users or administrators to review them and release or delete them as needed.

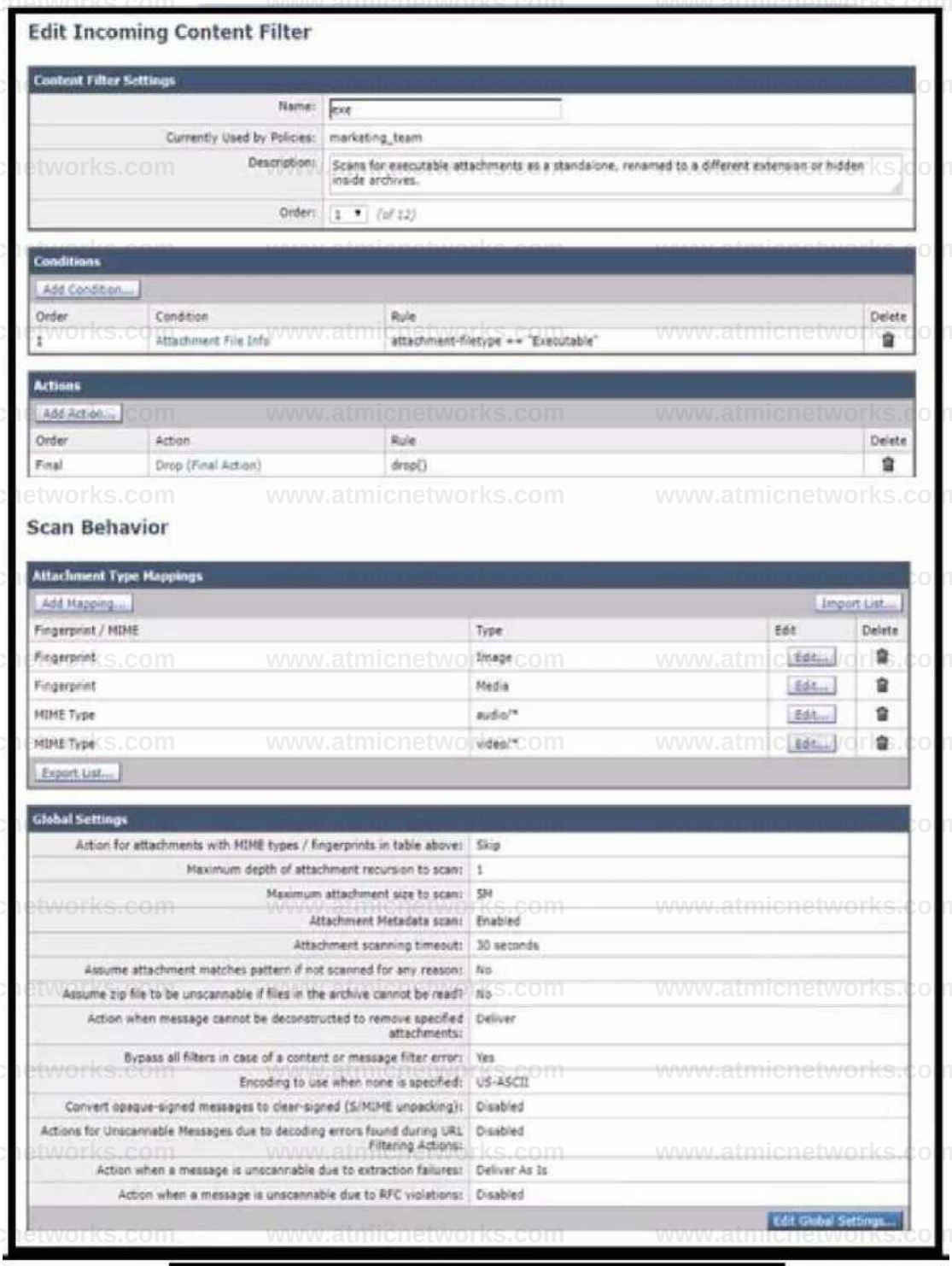
End users can access their personal spam quarantine on Cisco ESA either by clicking on a link in a notification email or by entering their email address and password in a web browser. In both cases, authentication is required to ensure security and privacy.

The other options are not valid restrictions that are in place for end users accessing the spam quarantine on Cisco Secure Email Gateway appliances, because they are either not mandatory or not related to authentication.

Reference: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 10-2 and page 10-3.

Question: 111

Refer to the exhibit.




```
Tue Aug 13 17:39:51 2019 Info: New SMTP ICID 391975 interface Management (10.66.71.122) address 10.137.84.196 reverse dns host unknown
verified no
Tue Aug 13 17:39:51 2019 Info: ICID 391975 ACCEPT SG UNKNOWNLIST match abra[none] SBRS rfc1918 country not applicable
Tue Aug 13 17:39:51 2019 Info: Start MID 379145 ICID 391975
Tue Aug 13 17:39:51 2019 Info: MID 379145 ICID 391975 From: <matt@lee.com>
Tue Aug 13 17:39:51 2019 Info: MID 379145 ICID 391975 RID 0 To: <bob_doe@cisco.com>
Tue Aug 13 17:39:54 2019 Info: MID 379145 Message-ID '<cp.z6f4nirfuxysu2@mathuynh-f645d.mshome.net>'
Tue Aug 13 17:39:54 2019 Info: MID 379145 Subject 'IMPORTANT ATTACHMENT PLEASE OPEN'
Tue Aug 13 17:39:55 2019 Info: MID 379145 ready 3917905 bytes from <matt@lee.com>
Tue Aug 13 17:39:55 2019 Info: MID 379145 matched all recipients for per-recipient policy marketing_team in the inbound table
Tue Aug 13 17:39:55 2019 Info: ICID 391975 close
Tue Aug 13 17:39:55 2019 Info: graymail [RPC_CLIENT] Graymail scan skipped since message size exceeds configured threshold
Tue Aug 13 17:39:55 2019 Info: MID 379145 was too big (3917905/524288) for scanning by Outbreak Filters
Tue Aug 13 17:39:55 2019 Info: MID 379145 was too big (3917905/2097152) for scanning by CASE
Tue Aug 13 17:39:57 2019 Info: MID 379145 using engine: GRAYMAIL negative
Tue Aug 13 17:39:57 2019 Info: MID 379145 attachment 'dangerous_file.zip'
Tue Aug 13 17:39:57 2019 Warning: MID 379145, Message Scanning Problem: Scan Depth Exceeded
Tue Aug 13 17:39:57 2019 Info: MID 379145 queued for delivery
```

Which configuration allows the Cisco Secure Email Gateway to scan for executables inside the archive file and apply the action as per the content filter?

A. Configure the recursion depth to a higher value.

B. Modify the content filter to look for attachment filetype of compressed.
C. Configure the maximum attachment size to a higher value.
D. Modify the content filter to look for exe filename instead of executable filetype.

Answer: A

Explanation:

The recursion depth is the number of levels that the Cisco Secure Email Gateway will scan inside an archive file for executables and other file types. If the recursion depth is too low, some executables may not be detected and scanned by the content filter. To allow the appliance to scan for executables inside the archive file and apply the action as per the content filter, you need to configure the recursion depth to a higher value1. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring File Reputation Filtering and File Analysis [Cisco Secure Email Gateway] - Cisco

Question: 112

Spammers routinely try to send emails with the recipient field filled with a list of all possible combinations of letters and numbers. These combinations, appended with a company domain name are malicious attempts at learning all possible valid email addresses. Which action must be taken on a Cisco Secure Email Gateway to prevent this from occurring?

A. Select the SMTP Authentication Query checkbox
B. Perform LDAP acceptance validation.
C. Quarantine external authentication queries.
D. Enable end user safelist features

Answer: B

Explanation:

LDAP acceptance validation is a feature that allows the Cisco Secure Email Gateway to check if the recipient address of an incoming message exists in an LDAP directory before accepting it. This feature can help prevent spammers from sending emails with invalid recipient addresses and reduce the load on the appliance2. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring LDAP Queries [Cisco Secure Email Gateway] - Cisco

Question: 113

A Cisco Secure Email Gateway appliance is processing many messages that are sent to invalid recipients verification. Which two steps are required to accomplish this task? (Choose two.)

A. Enable external LDAP authentication
B. Configure the LDAP query on a listener
C. Configure LDAP server profiles
D. Enable LDAP authentication on a listener
E. Configure incoming mail policy to query LDAP server

Answer: B, C

Explanation:

To enable LDAP recipient verification on a Cisco Secure Email Gateway appliance, you need to configure the LDAP query on a listener and configure LDAP server profiles. The LDAP query specifies the criteria for matching recipient addresses against an LDAP directory. The LDAP server profile defines the connection settings and authentication credentials for accessing an LDAP server2. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring LDAP Queries [Cisco Secure Email Gateway] - Cisco

Question: 114

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

A. Use the serial or console port
B. Use the management port
C. Use the data 2 port
D. Use the data 1 port

Answer: A

Explanation:

If you are unable to access the user interface of the Cisco Secure Email Gateway appliance after manipulating the subnet mask, you can use the serial or console port to perform the initial configuration. The serial or console port provides a command-line interface that allows you to configure basic network settings such as IP address, subnet mask, gateway, and hostname3. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring Network Settings [Cisco Secure Email Gateway] - Cisco

Question: 115

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

A. The sender is included in an ISP blocklist
B. Administrative access is required to create a safelist.
C. The sender didn't mark the message as urgent
D. End-user safelists apply to antispam engines only.

Answer: D

Explanation:

The reason why the CEO did not receive an important message expected from a trusted sender after adding them to a safelist is because end-user safelists apply to antispam engines only. End-user safelists are lists of sender addresses or domains that end users can create and manage through their quarantine accounts or email clients. End-user safelists allow end users to accept or exempt messages from certain senders or domains from being identified as spam by the antispam engines. However, end-user safelists do not affect other filtering engines such as antivirus, outbreak filters, or content filters. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Safelists and Blocklists [Cisco Secure Email Gateway] - Cisco

Question: 116

A company has recently updated their security policy and now wants to drop all email messages larger than 100 MB coming from external sources. The Cisco Secure Email Gateway is LDAP integrated and all employee accounts are in the group "Employees". Which filter rule configuration provides the desired outcome?

A. if (mail-from-group == 'Employees') and (body-size > "100M") {drop()}
B. if (mail-from-group != 'Employees') and (body-size > 100M) {drop();}
C. if (mail-from-group == 'Employees') and (body-size > 100M) {bounce();}
D. if ('mail-from-group != Employees') and (body-size > 100M) {drop();}

Answer: A

Explanation:

Question: 117

The CEO sent an email indicating that all emails containing a string of 123ABCDEFGHJ cannot be delivered and must be sent into quarantine for further inspection. Given the requirement, which regular expression should be used to match on that criteria?

A. \\D{3}[A-Z]{9}
B. \d{3}[A-Z]{9}
C. \W{3}[A-Z]{9}
D. {3}\d{9}[A-Z]

Answer: B

Explanation:

A regular expression is a sequence of characters that defines a search pattern for text. To match a string of 123ABCDEFGHJ, you need to use the following regular expression: \d{3}[A-Z]{9}. This expression means that the string must start with three digits (\d{3}), followed by nine uppercase letters ([A-Z]{9}). This expression will match any string that has the same format as 123ABCDEFGHJ. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Regular Expressions [Cisco Secure Email Gateway] - Cisco

Question: 118

A Cisco Secure Email Gateway administrator must provide outbound email authenticity and configures a DKIM signing profile to handle this task. What is the next step to allow this organization to use DKIM for their outbound email?

A. Enable the DKIM service checker
B. Export the DNS TXT record to provide to the DNS registrar
C. Import the DNS record of the service provider into the Cisco Secure Email Gateway.
D. Configure the Trusted Sender Group message authenticity policy.

Answer: B

Explanation:

To use DKIM for outbound email, the administrator must export the DNS TXT record from the Cisco Secure Email Gateway and provide it to the DNS registrar of the domain. This will allow the recipient servers to verify the DKIM signature of the email by querying the DNS record of the sender domain. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring DKIM Signing]

Question: 119

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?

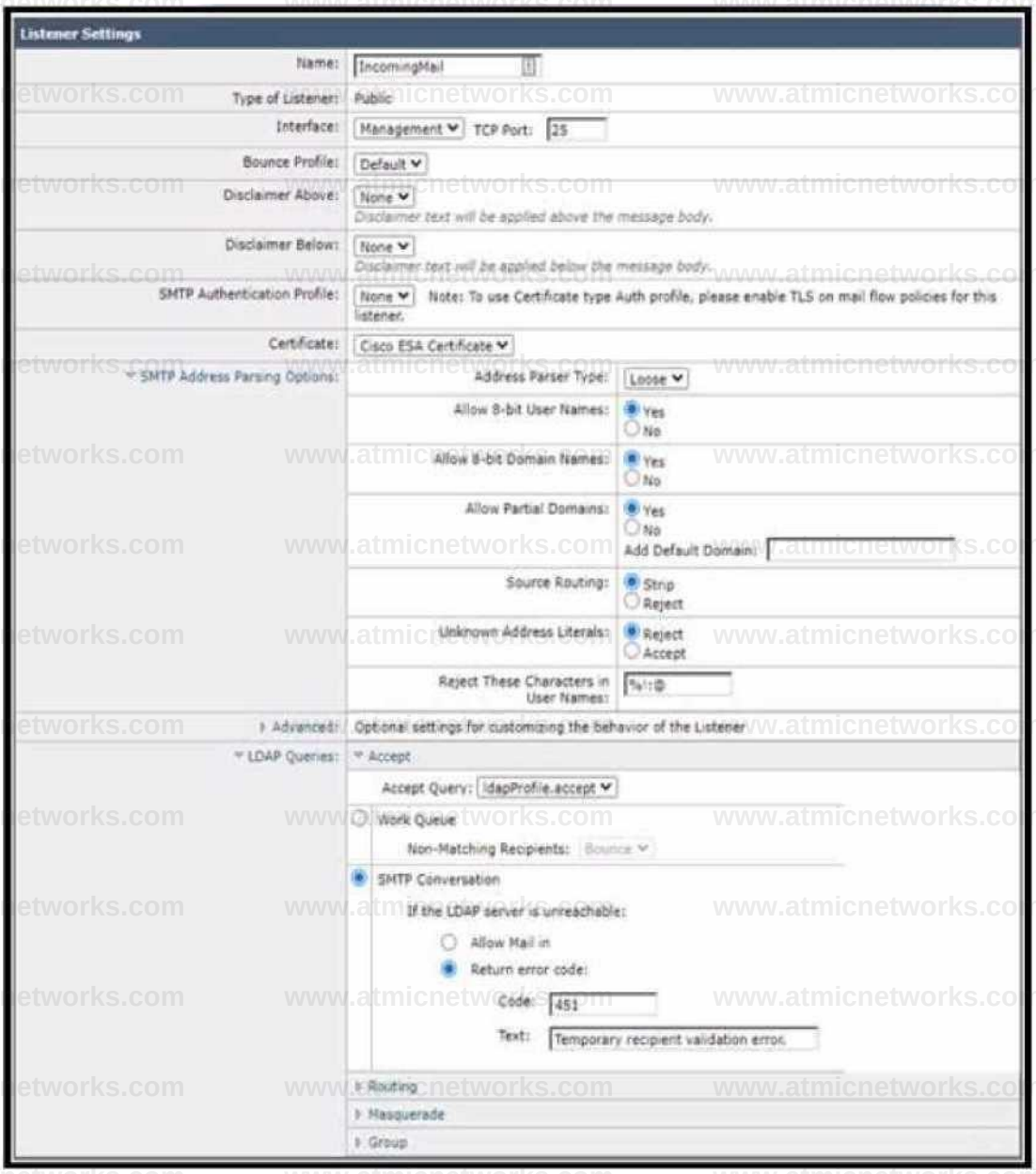
A. Action is skipping all antivirus checks for the mail
B. Action is applied to all mail that has the subject "FW: Bounce Notification."
C. Action is applied to all mail from test@cisco.com.
D. Action is skipping all antispam checks for the mail.

Answer: A

Explanation:

Question: 120

Refer to the exhibit.



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

Answer: C

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: 121

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

Answer: C

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: 122

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

Answer: B

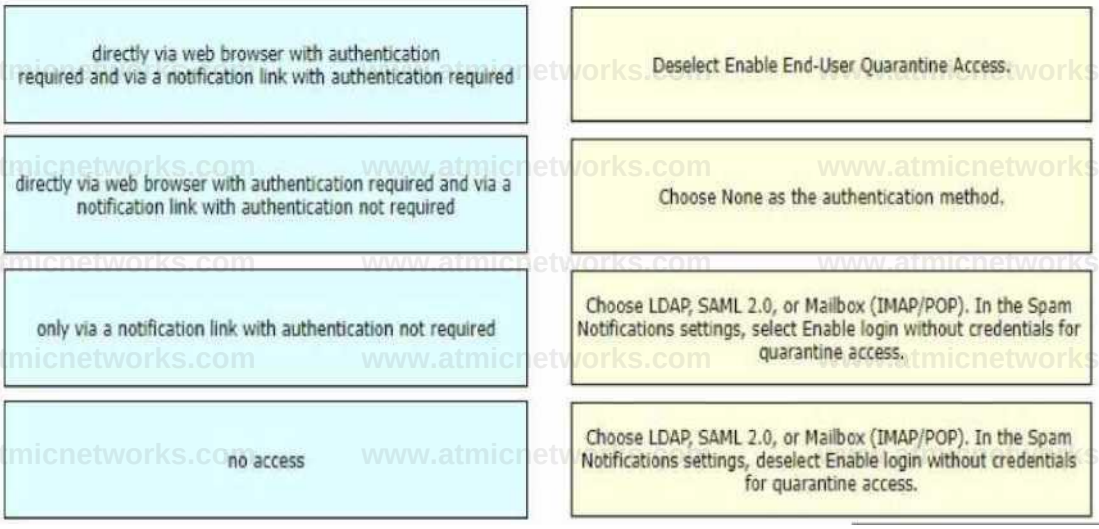
Explanation:

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: 123

DRAG DROP

Drag and drop authentication options for End-User Quarantine Access from the left onto the corresponding configuration steps on the right.



Answer:

Explanation:

Question: 124

A network administrator enabled McAfee antivirus scanning on a Cisco Secure Email Gateway and configured the virus scanning action of "scan for viruses only" If the scanner finds a virus in an attachment for an incoming email, what action will be applied to this message?

A. The email and attachment are forwarded to the network administrator.

B. No repair is attempted, and the attachment is either dropped or delivered C. The attachment is dropped and replaced with a "Removed Attachment" file D. The system will attempt to repair the attachment

Answer: B

Explanation:

If the McAfee antivirus scanning is enabled on the Cisco Secure Email Gateway and the virus scanning action is set to “scan for viruses only”, then no repair is attempted, and the attachment is either dropped or delivered based on the antivirus policy settings. The administrator can choose to drop or deliver the infected attachment by selecting the appropriate action in the antivirus policy. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring McAfee Antivirus Scanning]

Question: 125

What is a benefit of deploying Cisco Secure Email and Web Manager?

A. centralized management of software updates for Cisco Secure Email Gateway
B. centralized management of logs for Cisco Secure Email Gateway
C. centralized management of quarantined email
D. centralized management of botnet directories

Answer: C

Explanation:

One of the benefits of deploying Cisco Secure Email and Web Manager is that it provides centralized management of quarantined email for multiple Cisco Secure Email Gateway appliances. The administrator can use the Cisco Secure Email and Web Manager to view, search, release, delete, or forward quarantined messages from a single web interface. Reference: [Cisco Secure Email and Web Manager User Guide - Configuring Centralized Spam Quarantine]

Question: 126

Which functionality is impacted if the assigned certificate under one of the IP interfaces is modified?

A. traffic between the Cisco Secure Email Gateway and the LDAP server
B. emails being delivered from the Cisco Secure Email Gateway
C. HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway
D. emails being received by the Cisco Secure Email Gateway

Answer: C

Explanation:

If the assigned certificate under one of the IP interfaces is modified, then the HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway will be impacted. The administrator must ensure that the certificate is valid and trusted by the browser or client that is

used to access the web user interface. Otherwise, the connection may fail or generate a warning message. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Certificates]

Question: 127

A trusted partner of an organization recently experienced a new campaign that was leveraging JavaScript attachments to trick users into executing malware. As a result, they created a local policy to deny messages with JavaScript attachments. Which action should the administrator of the organization take to ensure encrypted communications are delivered to the intended partner recipient?

A. Insert the X-PostX-Use-Script' header with a value of false to the encrypted messages
B. Select JavaScript-free' option within the Cisco Secure Email Encryption Service Add-in
C. Create an outgoing content filter and add the Encrypt and Deliver Nov/ action with Use-Script option deselected
D. Create a new encryption profile and deselect the 'Use-Script' envelope settings option.

Answer: D

Explanation:

According to the User Guide for Cisco Secure Email Encryption Service Add-In 1, the 'Use-Script' option allows you to use JavaScript in the encrypted message envelope. This option is enabled by default, but you can disable it if you want to send encrypted messages to recipients who have security policies that block JavaScript attachments[2, p. 14].

The other options are not valid because:

A. Inserting the X-PostX-Use-Script header with a value of false to the encrypted messages is not a supported feature of the Cisco Secure Email Encryption Service Add-in1.

B. Selecting JavaScript-free option within the Cisco Secure Email Encryption Service Add-in is not a valid option. The add-in does not have such an option1.

C. Creating an outgoing content filter and adding the Encrypt and Deliver Nov/ action with Use-Script option deselected is not possible. The Encrypt and Deliver Nov/ action does not have a Use-Script option[2, p. 13].

Question: 128

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

Answer: C

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: 129

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

Answer: A

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: 130

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

Answer: A, B

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: 131

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.

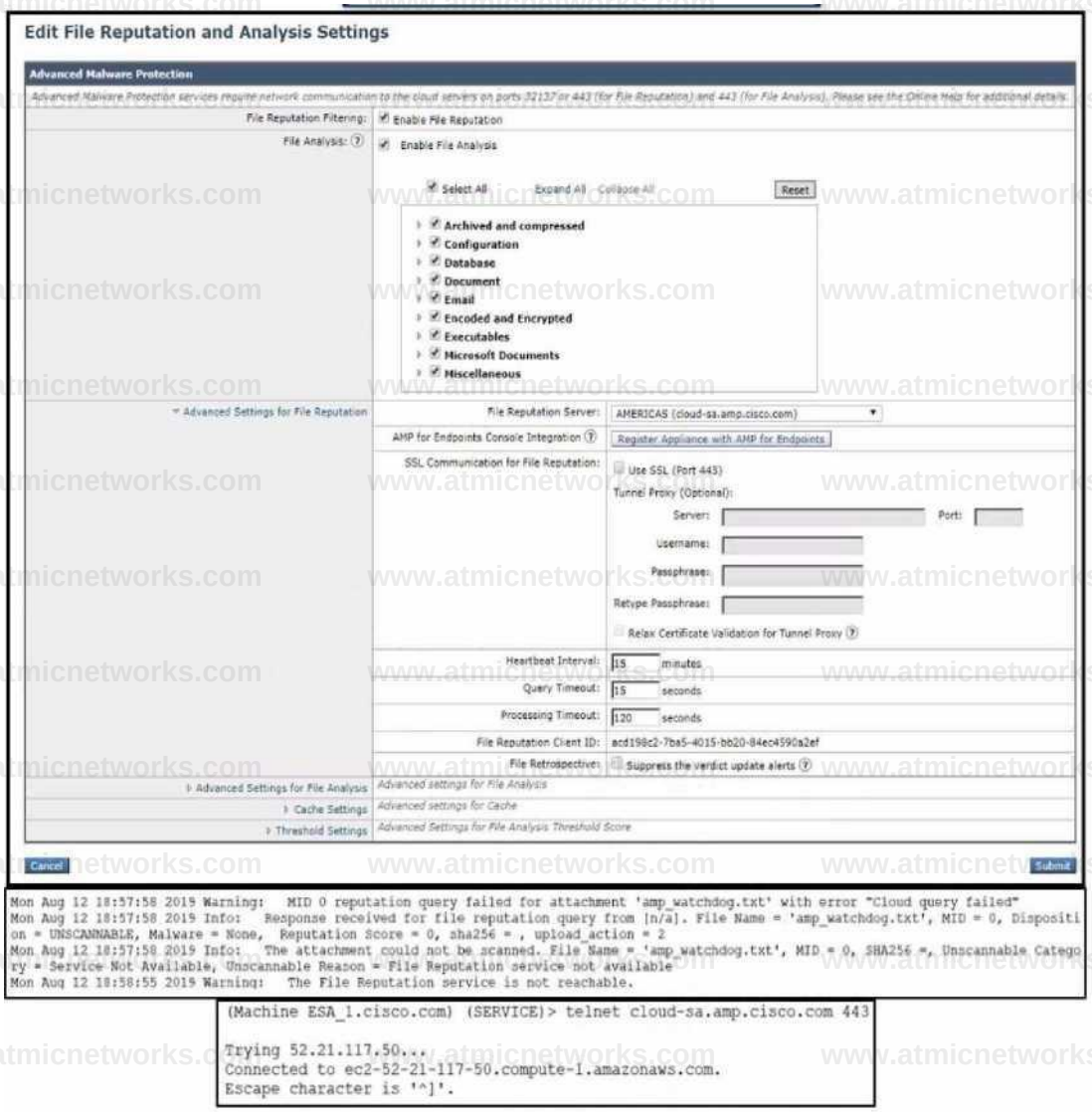
Answer: D, E

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]

Question: 132

Refer to the exhibit.



An administrator has configured File Reputation and File Analysis on the Cisco Secure Email Gateway appliance however it does not function as expected What must be configured on the appliance for this to function?

A. Upload the Root CA certificate for the File Reputation cloud to the Cisco Secure Email Gateway.
B. Open port 443 on the firewall for the Cisco Secure Email Gateway to connect to the File Reputation cloud.
C. Configure the Cisco Secure Email Gateway to use SSL for the connection to the File Reputation server
D. Restart the File Reputation service to force the scanning engine to connect to the File Reputation cloud.

Answer: C

Explanation:

To enable File Reputation and File Analysis on the Cisco Secure Email Gateway appliance, the administrator must configure the appliance to use SSL for the connection to the File Reputation server. This will ensure that the communication between the appliance and the cloud service is secure and encrypted. The administrator must also upload a valid certificate from a trusted CA on the

appliance for this purpose. The other options are not required or effective for this task. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring File Reputation and File Analysis]

Question: 133

Which action do Outbreak Filters take to stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites?

A. Rewrite URLs to redirect traffic to potentially harmful websites through a web security proxy
B. Block all emails from email domains associated with potentially harmful websites.
C. Strip all attachments from email domains associated with potentially harmful websites.
D. Quarantine messages that contain links to potentially harmful websites until the site is taken offline

Answer: A

Explanation:

Outbreak Filters can take the action of rewriting URLs to redirect traffic to potentially harmful websites through a web security proxy. This allows the Cisco Secure Email Gateway to scan the content of the websites and block or warn the user if they are malicious or undesirable. This action can stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites, that may not be detected by other filters. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Outbreak Filters]

Question: 134

What is the default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHCP server is not available?

A. Manual configuration of an IP address is required through the serial port before remote access
B. DHCP is required for the initial IP address assignment
C. Use the IP address of 192.168 42 42 via the Management port
D. Manual configuration of an IP address is required through the hypervisor console before remote access

Answer: C

Explanation:

The default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHCP server is not available is to use the IP address of 192.168.42.42 via the Management port. This IP address is assigned by default to the Management port of the virtual gateway and can be used to access the web user interface or the command-line interface of the appliance. Reference: [Cisco Secure Email Gateway Installation and Upgrade Guide - Configuring Network Settings]

Question: 135

An administrator notices that the Cisco Secure Email Gateway delivery queue on an appliance is

consistently full. After further investigation, it is determined that the IP addresses currently in use by appliance are being rate-limited by some destinations. The administrator creates a new interface with an additional IP address using virtual gateway technology, but the issue is not solved Which configuration change resolves the issue?

A. Use the CLI command altsrchost to set the new interface as the source IP address for all mail.

B. Use the CLI command loadbalance auto to enable mail delivery over all interfaces.
C. Use the CLI command alt-src-host to set the new interface as a possible delivery candidate.
D. Use the CLI command deliveryconfig to set the new interface as the primary interface for mail delivery

Answer: D

Explanation:

Determining Which Interface is Used for Mail Delivery Unless you specify the output interface via the deliveryconfig</code> command or via a message filter (alt-src-host), or through the use of a virtual gateway, the output interface is selected by the AsyncOS routing table.
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_011001.html?bookSearch =true

Question: 136

An engineer wants to ensure that emails received by company users that contain URLs do not make them susceptible to data loss from accessing malicious or undesired external content sources Which two features must be configured on Cisco Secure Email Gateway to meet this requirement1? (Choose two.)

A. antispam scanning
B. data loss prevention
C. graymail detection
D. URL filtering
E. antivirus scanning

Answer: A, D

Explanation:

To meet the requirement of ensuring that emails received by company users that contain URLs do not make them susceptible to data loss from accessing malicious or undesired external content sources, the administrator must configure two features on Cisco Secure Email Gateway: antispam scanning and URL filtering. Antispam scanning can block or quarantine messages that are identified as spam based on various criteria, such as sender reputation, message content, and message headers. URL filtering can rewrite or defang URLs in messages that are associated with malicious or undesirable websites, such as phishing, malware, adult, or gambling sites. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Antispam Scanning] and [Cisco Secure Email Gateway Administrator Guide - Configuring URL Filtering]

Question: 137

Which feature must be activated on a Cisco Secure Email Gateway to combat backscatter?

A. Graymail Detection
B. Bounce Verification
C. Forged Email Detection
D. Bounce Profile

Answer: B

Explanation:

To combat backscatter, which is a type of spam that consists of bounce messages sent to forged sender addresses, the administrator must enable the Bounce Verification feature under Security Settings. This feature allows the appliance to verify whether a bounce message is legitimate or not by checking if the original message was sent from the appliance. If not, the bounce message is considered as backscatter and can be dropped or quarantined. Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Bounce Verification]

Question: 138

Which Cisco Secure Email Threat Defense visibility and remediation mode is only available when using Cisco Secure Email Gateway as the message source?

A. Basic Authentication
B. No Authentication
C. Microsoft 365 Authentication
D. Cisco Security Cloud Sign On

Answer: B

Explanation:

According to the Cisco Secure Email Threat Defense User Guide, the No Authentication option is only available if you are using a Cisco Secure Email Gateway (SEG) as your message source. This option allows visibility only, no remediation1.

The other options are not valid because:

A. Basic Authentication is not a visibility and remediation mode for Cisco Secure Email Threat Defense. It is a method of authenticating users with a username and password2.

C. Microsoft 365 Authentication is a visibility and remediation mode that allows you to use Microsoft 365 credentials to access Cisco Secure Email Threat Defense. It has two sub-options: Read/Write and Read. This mode is available for both Microsoft 365 and Gateway message sources1.

D. Cisco Security Cloud Sign On is not a visibility and remediation mode for Cisco Secure Email Threat Defense. It is a service that manages user authentication for Cisco security products, including Cisco Secure Email Threat Defense3.

Question: 139

An engineer tries to implement phishing simul-ations to test end users, but they are being blocked by the Cisco Secure Email Gateway appliance. Which two components, when added to the allow list, allow these simul-ations to bypass antispam scanning? (Choose two.)

A. domains
B. senders
C. reputation score
D. receivers
E. spf check

Answer: A, B

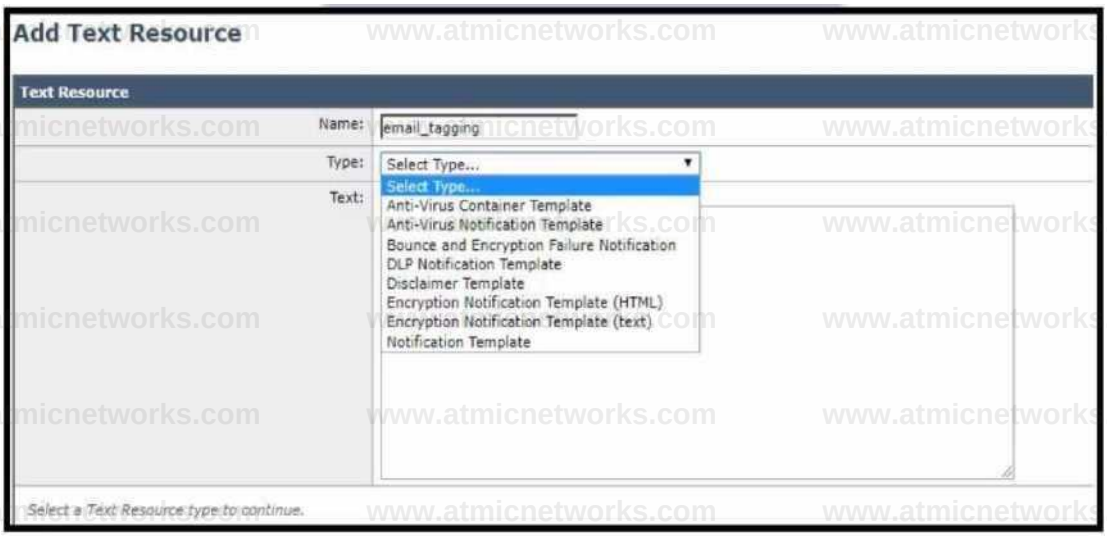
Explanation:

To allow phishing simul-ations to bypass antispam scanning, the administrator must add two components to the

allow list: domains and senders. Domains are the email domains that are used in the phishing simulations, such as example.com or test.com. Senders are the email addresses that are used to send the phishing simulations, such as phish@example.com or test@test.com. By adding these components to the allow list, the administrator can prevent them from being blocked by antispam scanning and allow them to reach the end users for testing purposes. Reference: [Cisco Secure Email Gateway Administrator Guide - Creating Allow Lists]

Question: 140

Refer to the exhibit.



For improved security, an administrator wants to warn users about opening any links or attachments within an email How must the administrator configure an HTML-coded message at the top of an email body to create this warning?

A. Create a text resource type of Disclaimer Template paste the HTML code into the text box. then use this text resource inside a content filter

B. Create a text resource type of Disclaimer Template change to code view to paste the HTML code into the text box, then use this text resource inside a content filter

C. Create a text resource type of Notification Template, paste the HTML code into the text box, then use this text resource inside a content filter.

D. Create a text resource type of Notification Template, change to code view to paste the HTML code into the text box. then use this text resource inside a content filter.

Answer: B

Explanation:

According to the [Cisco Secure Email User Guide], you can create a text resource of type Disclaimer Template and use the code view option to insert HTML code into the text box. Then, you can use this text resource in a content filter to prepend or append the HTML message to the email body[1, p. 1516].

The other options are not valid because:

A. Creating a text resource type of Disclaimer Template and pasting the HTML code into the text box without changing to code view will not work, as the HTML code will be treated as plain text and not rendered properly[1, p. 15].

C. Creating a text resource type of Notification Template and pasting the HTML code into the text box will not work, as Notification Templates are used for sending notifications to senders or recipients, not for modifying the email body[1, p. 17].

D. Creating a text resource type of Notification Template and changing to code view to paste the HTML code into the text box will not work, as Notification Templates are used for sending notifications to senders or recipients, not for modifying the email body[1, p. 17].

Question: 141

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

Answer: C, E

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 AddIn. 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 AddIn. 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: 142

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

Answer: D

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: 143

Which type of DNS record would contain the following line, which references the DKIM public key per RFC 6376?
v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A2362BECE406582670456943283BE

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

Answer: C

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: 144

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.

Answer: C

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: 145

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.

Answer: C

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: 146

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

Answer: C, D

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: 147

What is a category for classifying graymail?

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

Answer: B

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].