Free Questions for 300-720 by ebraindumps

Shared by Delaney on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.)

Options:

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 2

Question Type: MultipleChoice

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?

Options:

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

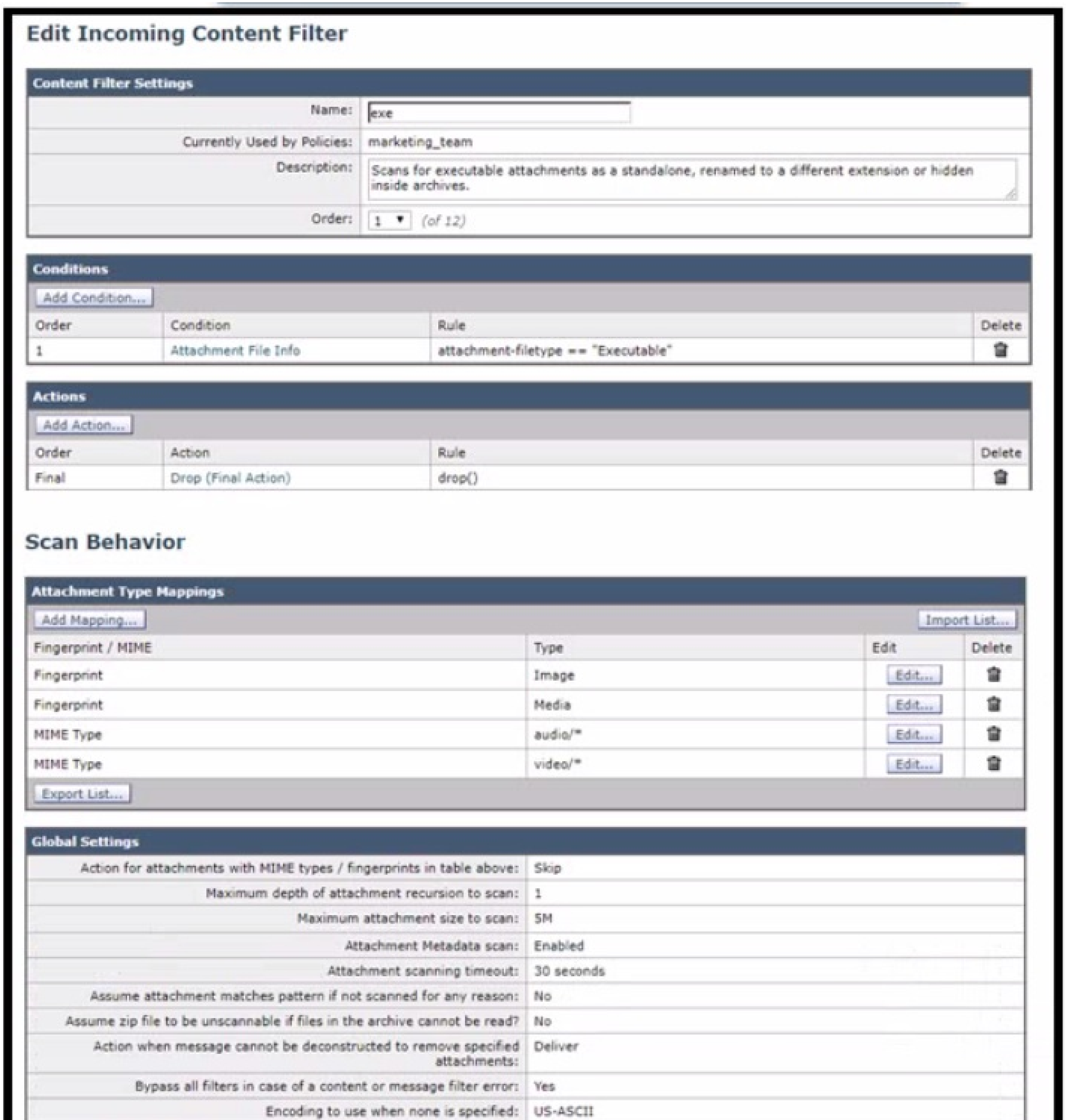
Explanation:

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 3

Question Type: MultipleChoice

Refer to the exhibit.



Edit Incoming Content Filter

Content Filter Settings

Name:	exe
Currently Used by Policies:	marketing_team
Description:	Scans for executable attachments as a standalone, renamed to a different extension or hidden inside archives.
Order:	1 ▼ *(of 12)*

Conditions

Order	Condition	Rule	Delete
1	Attachment File Info	attachment-filetype == "Executable"	🗑

Actions

Order	Action	Rule	Delete
Final	Drop (Final Action)	drop()	🗑

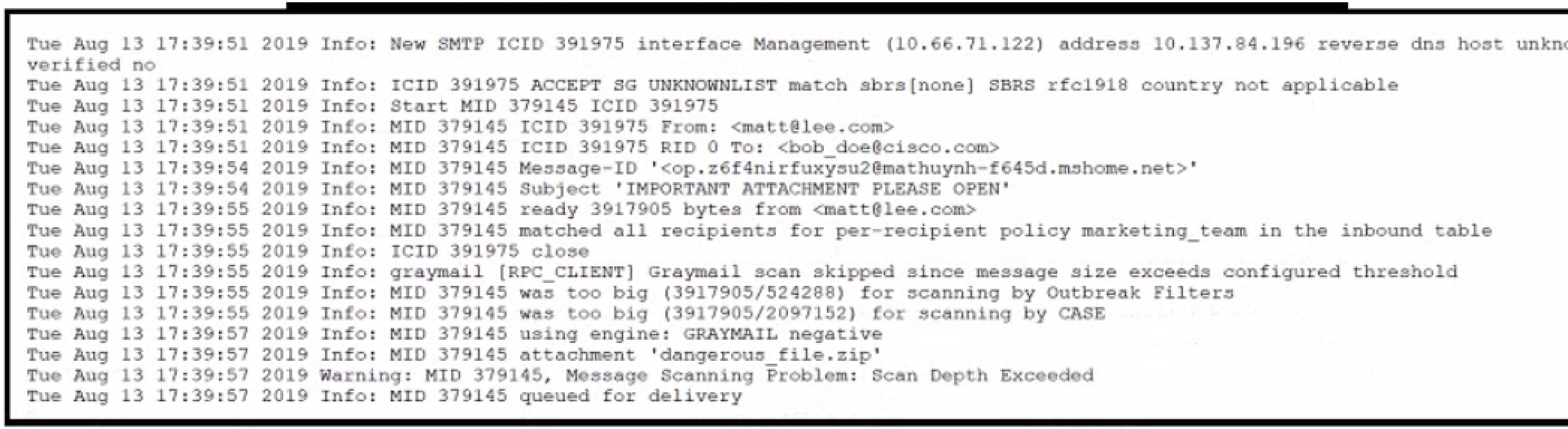
Scan Behavior

Attachment Type Mappings

Fingerprint / MIME	Type	Edit	Delete
Fingerprint	Image	Edit...	🗑
Fingerprint	Media	Edit...	🗑
MIME Type	audio/*	Edit...	🗑
MIME Type	video/*	Edit...	🗑

Global Settings

Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	1
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



```
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 unkn
verified no
Tue Aug 13 17:39:51 2019 Info: ICID 391975 ACCEPT SG UNKNOWNLIST match sbrs[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 '<op.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?

Options:

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 4

Question Type: MultipleChoice

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

Options:

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.

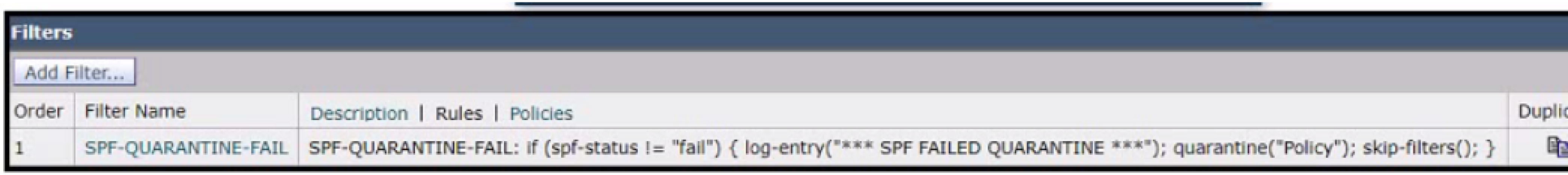
End users can access their personal spam quarantine on Cisco ESA either by clicking on a link in a notification email or by entering their email address and password in a web browser. In both cases, authentication is required to ensure security and privacy.

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.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



Order	Filter Name	Description | Rules | Policies	Duplic
1	SPF-QUARANTINE-FAIL	SPF-QUARANTINE-FAIL: if (spf-status != "fail") { log-entry("*** SPF FAILED QUARANTINE ***"); quarantine("Policy"); skip-filters(); }	

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?

Options:

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.

Question 6

Question Type: MultipleChoice

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?

Options:

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.

Question 7

Question Type: MultipleChoice

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?

Options:

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 8

Question Type: MultipleChoice

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

Options:

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.

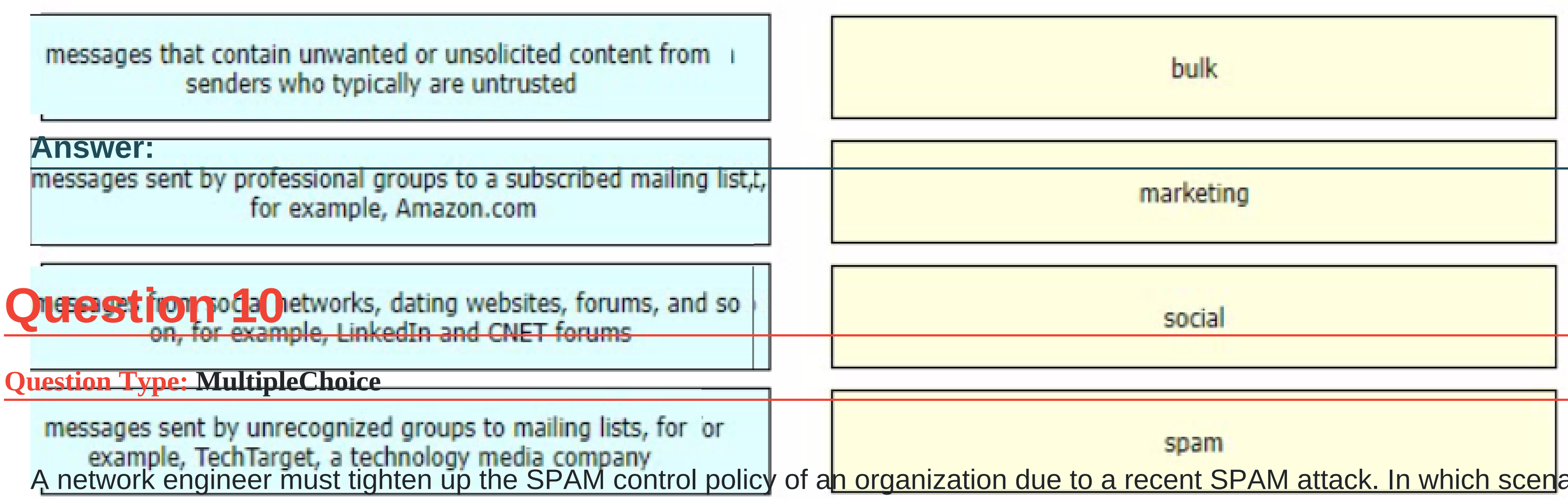
Enter the email address of the CEO, such as ceo@example.com.

Click Submit.

Question 9

Question Type: DragDrop

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



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

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

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

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

Answer:

Question 10

Question Type: MultipleChoice

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?

Options:

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 11

Question Type: MultipleChoice

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?

Options:

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.