# Cisco 300-720 Mock Exam

**Shared by Beach on 17-06-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

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

## Options:

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



## Answer:

C, E

## 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).

# Question 2

Question Type: MultipleChoice

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?

## Options:

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 3

Question Type: MultipleChoice

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?

## Options:

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 4

Question Type: MultipleChoice

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?

### Options:

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 5

Question Type: MultipleChoice

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?

## Options:

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.

# Question 6

Question Type: MultipleChoice

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?

## Options:

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

# Question 7

Question Type: MultipleChoice

How does the graymail safe unsubscribe feature function?

## Options:

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

## Question 8

Question Type: MultipleChoice

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

### Options:

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 9

Question Type: MultipleChoice

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

## Options:

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.

# Question 10

Question Type: MultipleChoice

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.)

## Options:

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 Add-In. The websafe portal allows you to compose and send encrypted messages from any web browser, while the Cisco Secure Email Add-In allows you to encrypt messages from your email client such as Outlook[2, p. 6-7].

B) This feature allows users to send up to 100MB of attachments in a secure email, not 50MB[2, p. 9].

D) Large file attachments can be sent using both the websafe portal and the Cisco Secure Email Add-In. The websafe portal allows you to compose and send encrypted messages from any web browser, while the Cisco Secure Email Add-In allows you to encrypt messages from your email client such as Outlook[2, p. 6-7].

# Question 11

Question Type: MultipleChoice

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?

## Options:

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.

# Question 12

Question Type: MultipleChoice

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

## Options:

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.



P2P exams