

[Q49-Q67 Free Sales Ending Soon - Use Real 300-720 PDF Questions [Dec 08, 2023]



Free Sales Ending Soon - Use Real 300-720 PDF Questions [Dec 08, 2023]  
Updated Dec-2023 Exam 300-720 Dumps - Pass Your Certification Exam

#### QUESTION 49

Which two statements about configuring message filters within the Cisco ESA are true? (Choose two.)

- \* The filters command executed from the CLI is used to configure the message filters.
- \* Message filters configuration within the web user interface is located within Incoming Content Filters.
- \* The filterconfig command executed from the CLI is used to configure message filters.
- \* Message filters can be configured only from the CLI.
- \* Message filters can be configured only from the web user interface.

Reference:

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

#### QUESTION 50

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

- \* message filter
- \* antivirus scanning
- \* outbreak filter
- \* antispam scanning

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.

## QUESTION 51

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?

- \* file reputation filtering
- \* outbreak filtering
- \* data loss prevention
- \* file analysis

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

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

## QUESTION 52

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

- \* The default engine scans for viruses first and the McAfee engine scans for viruses second.
- \* The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.
- \* The McAfee engine scans for viruses first and the default engine scans for viruses second.
- \* The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.

Explanation

If you configure multi-layer anti-virus scanning, the Cisco appliance performs virus scanning with the McAfee engine first and the Sophos engine second. It scans messages using both engines, unless the McAfee engine detects a virus. If the McAfee engine detects a virus, the Cisco appliance performs the anti-virus actions (repairing, quarantining, etc.) defined for the mail policy.

## QUESTION 53

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

- \* Add a DLP policy on the Incoming Mail Policy.
- \* Add a DLP policy to the DLP Policy Manager.
- \* Enable a DLP policy on the Outgoing Mail Policy.
- \* Enable a DLP policy on the DLP Policy Customizations.
- \* Add a DLP policy to the Outgoing Content Filter.

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user\\_guide/](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 54

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

```
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 RID o To: <bob_doe@cisco.com>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Message-ID '<op.z6f2luf7uxysu20mathuynh-f645d.mshome.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: MID 379133 matched all recipients for pre-recipient policy marker team in the inbound table
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/524208) for scanning by Outbound Filters
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/2097152) for scanning by CSE
Tue Aug 13 16:55:50 2019 Info: MID 379133 interim AV verdict using Sophos: CLEAN
Tue Aug 13 16:55:50 2019 Info: MID 379133 antivirus negative
Tue Aug 13 16:55:50 2019 Info: MID 379133 using engine: Sophos: Negative
Tue Aug 13 16:55:52 2019 Info: MID 379133 attachment id 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

Attachment Type Mappings			
Add Mapping...			
Fingerprint/MIME	Type	Edit	Delete
Fingerprint	Image	Edit...	
Fingerprint	Media	Edit...	
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
Export List...			

## 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...

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

**QUESTION 55**

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

- \* 8025
- \* 6443
- \* 6025
- \* 8443

Reference:

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

**QUESTION 56**

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

- \* 8025
- \* 6443
- \* 6025
- \* 8443

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.

**QUESTION 57**

DRAG DROP

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

Select and Place:

drop

encrypt messages

quarantine

deliver

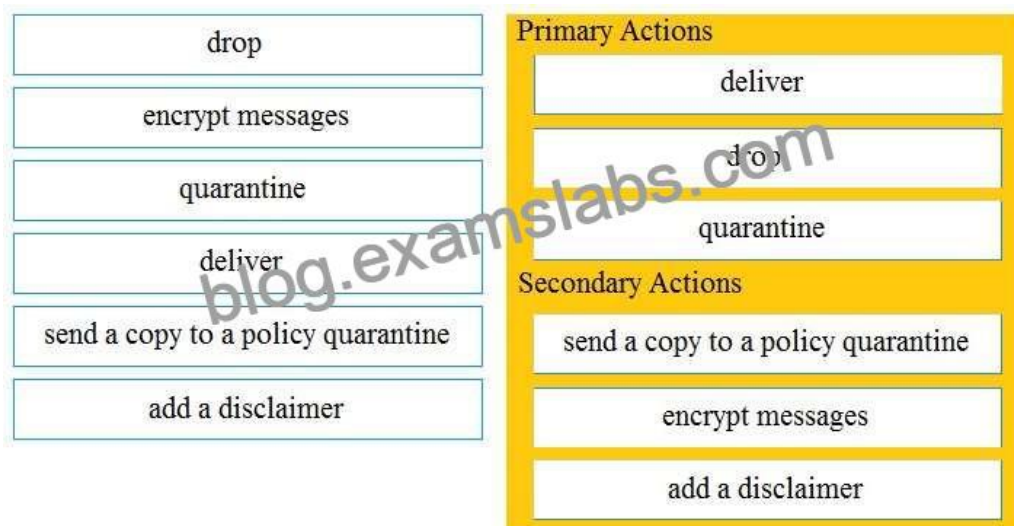
send a copy to a policy quarantine

add a disclaimer

Primary Actions

Secondary Actions





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](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 58

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?

- \* The retention period was changed to one hour.
- \* The threshold settings were set to override the clock settings.
- \* The retention period was set to default.
- \* The threshold settings were set to default.

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](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 59

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

- \* Enable outbreak filters.
- \* Enable email relay.
- \* Enable antispam scanning.
- \* Enable port bouncing.
- \* Enable antivirus scanning.

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](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 60

Mail Policies: Advanced Malware Protection	
<b>Advanced Malware Protection Settings</b>	
<b>Policy:</b>	DEFAULT
<b>Enable Advanced Malware Protection for This Policy:</b>	<input type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> No
<b>Message Scanning</b>	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
<b>Unscannable Actions on Message Errors</b>	
Action Applied to Message:	Deliver As Is ▼
▸ Advanced	Optional settings for custom header and message delivery.
<b>Unscannable Actions on Rate Limit</b>	
Action Applied to Message:	Deliver As Is ▼
▸ Advanced	Optional settings for custom header and message delivery.
<b>Unscannable Actions on AMP Service Not Available</b>	
Action Applied to Message:	Deliver As Is ▼
▸ Advanced	Optional settings for custom header and message delivery.
<b>Messages with Malware Attachments:</b>	
Action Applied to Message:	Drop Message ▼
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: MALWARE DETECTED]
▸ Advanced	Optional settings.
<b>Messages with File Analysis Pending:</b>	
Action Applied to Message:	Deliver As Is ▼
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: ATTACHMENT(S) MAY CONTAIN MA
▸ Advanced	Optional settings.

Refer to the exhibit. How should this configuration be modified to stop delivering Zero Day malware attacks?

- \* Change Unscannable Action from Deliver As Is to Quarantine.
- \* Change File Analysis Pending action from Deliver As Is to Quarantine.
- \* Configure mailbox auto-remediation.

- \* Apply Prepend on Modify Message Subject under Malware Attachments.

### QUESTION 61

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

- \* 20 MB
- \* 25 MB
- \* 15 MB
- \* 30 MB

### QUESTION 62

Which attack is mitigated by using Bounce Verification?

- \* spoof
- \* denial of service
- \* eavesdropping
- \* smurf

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

### QUESTION 63

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

- \* denial of service
- \* zero-day
- \* backscatter
- \* phishing

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\\_010000.html#con\\_1809885](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 64

Which benefit does enabling external spam quarantine on Cisco SMA provide?

- \* ability to back up spam quarantine from multiple Cisco ESAs to one central console
- \* access to the spam quarantine interface on which a user can release, duplicate, or delete
- \* ability to scan messages by using two engines to increase a catch rate
- \* ability to consolidate spam quarantine data from multiple Cisco ESA to one central console

### QUESTION 65

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

- \* The default engine scans for viruses first and the McAfee engine scans for viruses second.
- \* The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.
- \* The McAfee engine scans for viruses first and the default engine scans for viruses second.
- \* The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.

[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\\_010111.html](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_010111.html) According to the User Guide for AsyncOS 12.0 for Cisco Email Security Appliances<sup>2</sup>, 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 66

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

- \* message filter
- \* antivirus scanning
- \* outbreak filter
- \* antispam scanning

### QUESTION 67

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

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

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 Email.

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].

What is the amount for Cisco 300-720 Exam - The price of the Cisco 300-720 Exam is \$300 USD.



Cisco 300-720 certification exam is part of the Cisco Certified Specialist - Email Content Security certification. Securing Email with Cisco Email Security Appliance certification is an excellent way to showcase your expertise in email security technologies and solutions. The Cisco Email Security Appliance is a widely used email security solution that is used by many organizations worldwide. By passing this certification exam, you will be able to demonstrate your proficiency in email security technologies and solutions and enhance your career prospects in the cybersecurity field.

**300-720 Dumps To Pass CCNP Security Exam in One Day:**

<https://www.examlabs.com/Cisco/CCNP-Security/best-300-720-exam-dumps.html>]