300-720 Q&As

Securing Email with Cisco Email Security Appliance (SESA)

Pass Cisco 300-720 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-720.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

What is the cause of this error?

A. Content filters are configured at the machine-level on esa1.

B. DLP is configured at the cluster-level on esa2.

C. DLP is configured at the domain-level on esa1.

D. DLP is not configured on host1.

Correct Answer: D

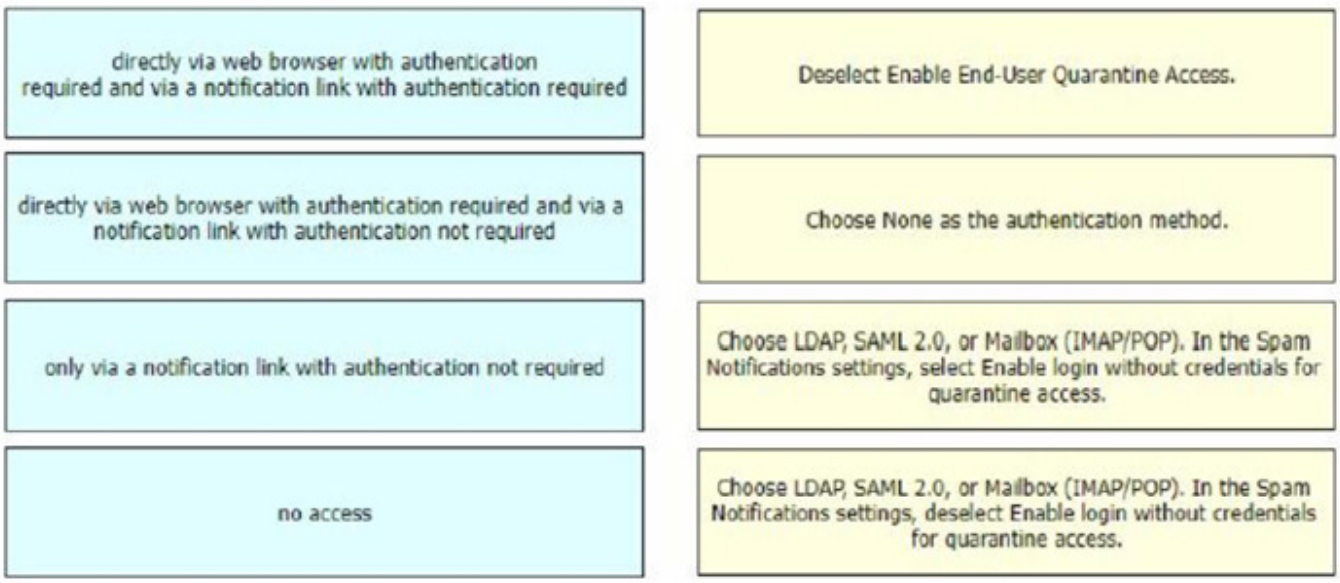
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html

QUESTION 2

DRAG DROP

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

Select and Place:



Correct Answer:

QUESTION 3

What is a category for classifying graymail?

A. Priority

B. Marketing

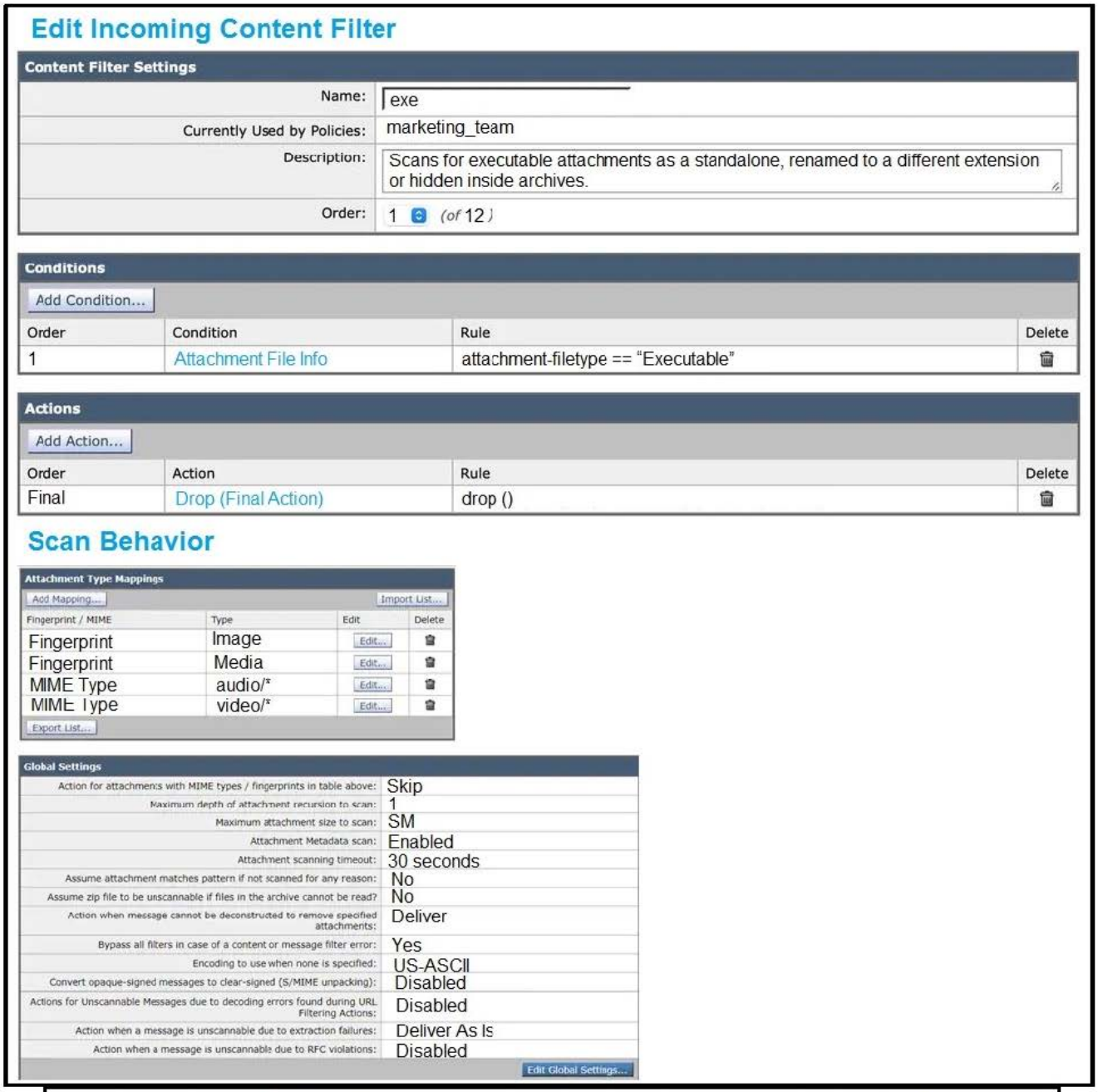
C. Malicious

D. Spam

Correct Answer: B

QUESTION 4

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

Add Condition...

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

Actions

Add Action...

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

Scan Behavior

Attachment Type Mappings

Add Mapping... Import List...

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:	1
Maximum attachment size to scan:	SM
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...

```
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 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 ESA to scan for executables inside the zip and apply the action as per the content filter?

A. Modify the content filter to look for .exe filename instead of executable filetype.

B. Configure the recursion depth to a higher value.

C. Configure the maximum attachment size to a higher value.

D. Modify the content filter to look for attachment filetype of compressed.

Correct Answer: C

QUESTION 5

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

A. Show the SLBL cache on the CLI.

B. Monitor Incoming/Outgoing Listener.

C. Export the SLBL to a .csv file.

D. Debug the mail flow policy.

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117922-technote-esa-00.html