300-720Q&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.leads4pass.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 notices that the Cisco ESA delivery queue is consistently full. After further investigation, it is determined that the IP addresses currently in use by the Cisco ESA 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 alt-src-host to set the new interface as a possible delivery candidate.

B. Use the CLI command loadbalance auto to enable mail delivery over all interfaces.

C. Use the CLI command deliveryconfig to set the new interface as the primary interface for mail delivery.

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

Correct Answer: B

QUESTION 2

An organization wants to prevent proprietary patent documents from being shared externally via email. The network administrator reviewed the DLP policies on the Cisco ESA 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. regulatory compliance

B. acceptable use

C. custom policy

D. privacy protection

Correct Answer: D

QUESTION 3

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

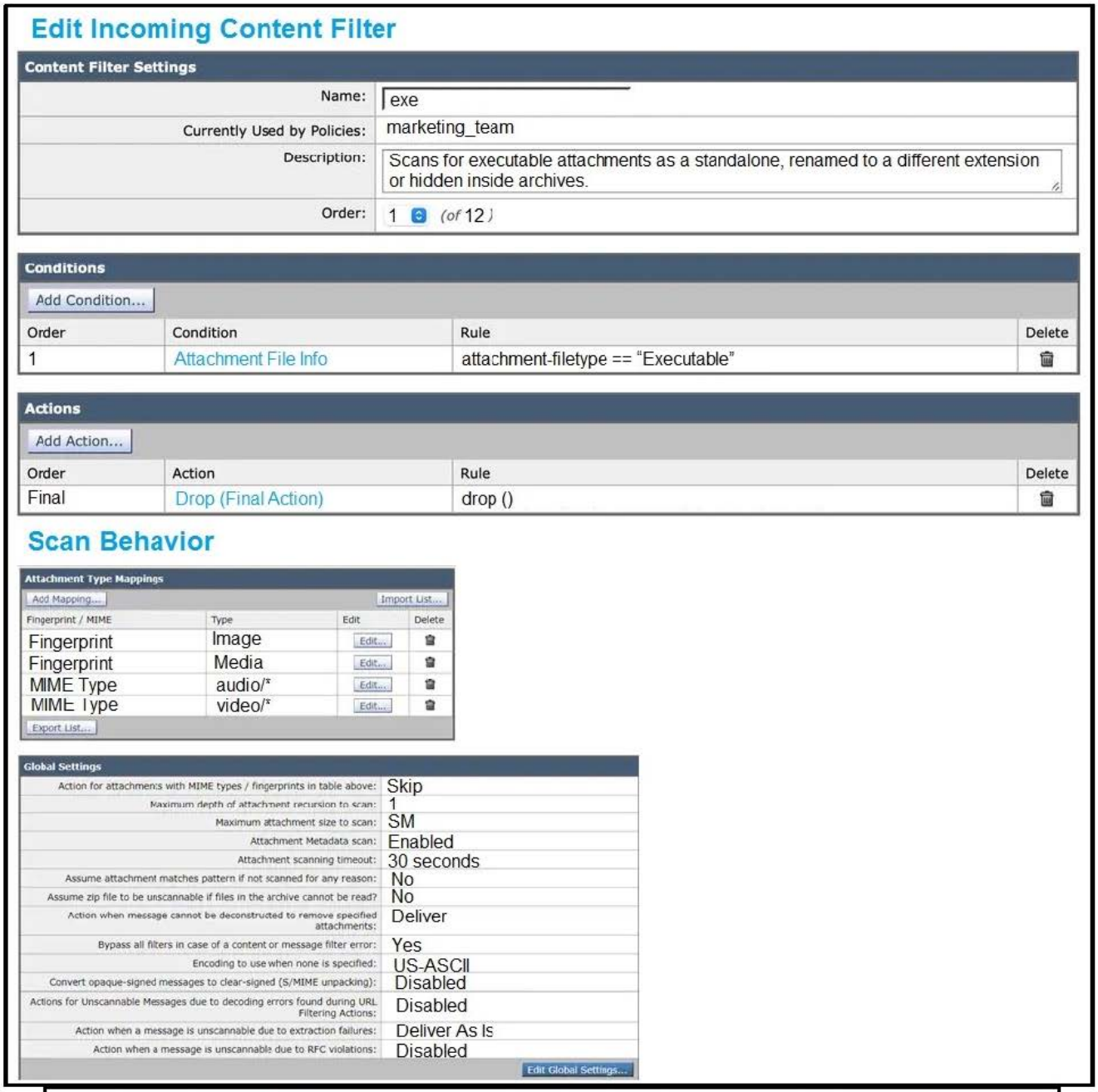
D. Entity ID

Correct Answer: A

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 4

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 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

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

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa-configure-dkim-signing.html

QUESTION 6

A network engineer is implementing a virus outbreak filter on a Cisco ESA by using the Outbreak Filters feature with plans to perform an additional scan by using a content filter. Which action must be taken by the Outbreak Filters?

A. Scan processed messages by using two engines simultaneously.

B. Send a copy of messages to quarantine.

C. Send processed messages to the Cisco ESA.

D. Scan processed messages by using a secondary instance of the Cisco ESA.

Correct Answer: C

QUESTION 7

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

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214269-filter-to-handle-messages-that-skipped-d.html

QUESTION 8

Refer to the exhibit.

Num	Active	Valid	Name
1	Y	Y	Anti_Spoofing
2	N	Y	Skip-filter
3	Y	Y	WHITELIST

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

Correct Answer: D

QUESTION 9

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.

Correct Answer: DE

QUESTION 10

Refer to the exhibit.

```
TEST: if (forged-email-detection ("support", 60)) { fed("from", ""); }
```

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 "TEST" to "Executives".

C. Change "fed" to "Executives".

D. Change "support" to "Executives".

Correct Answer: D

QUESTION 11

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?

A. ceo

B. Example CEO

C. ceo@example.com

D. example.com

Correct Answer: C

QUESTION 12

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.

Correct Answer: D

QUESTION 13

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

Correct Answer: AE

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 14

An organization has multiple Cisco ESA devices deployed, resulting in several spam quarantines to manage. To manage the quarantined messages, the administrator enabled the centralized spam quarantine on the Cisco SMA and configured the external spam quarantine on the Cisco ESA devices. However, messages are still being directed to the local quarantine on the Cisco ESA devices. What change is necessary to complete the configuration?

A. Modify the incoming mail policies on the Cisco ESA devices to redirect to the external quarantine.

B. Disable the external spam quarantine on the Cisco ESA devices.

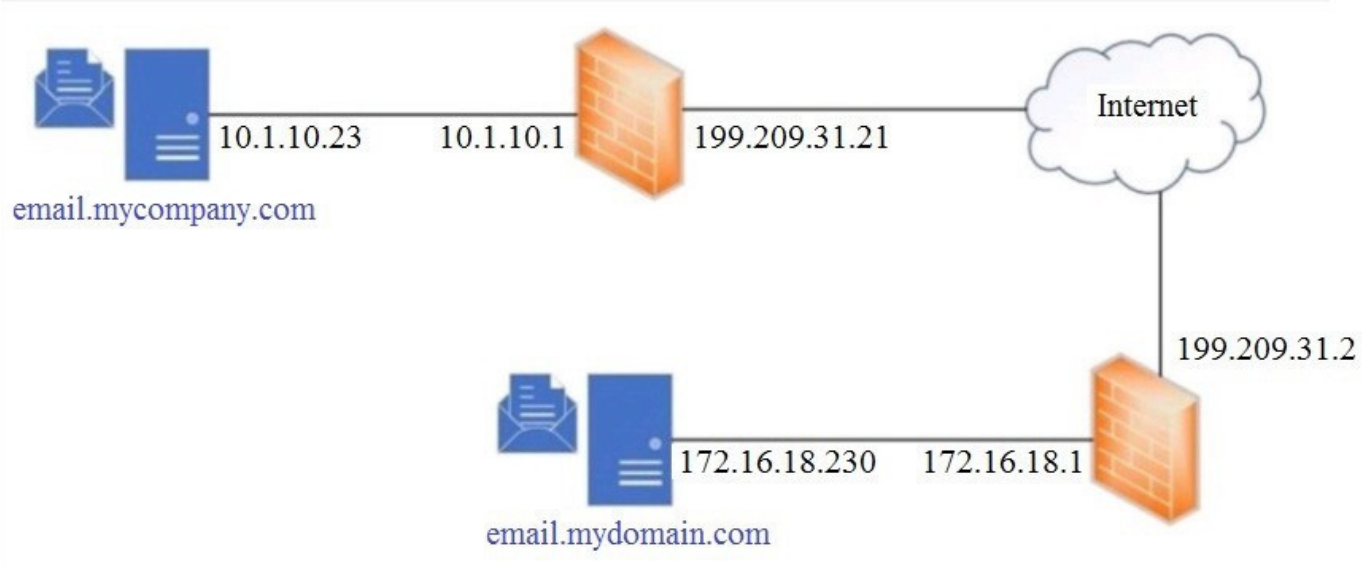
C. Disable the local spam quarantine on the Cisco ESA devices.

D. Modify the external spam quarantine settings on the Cisco ESA devices and change the port to 25.

Correct Answer: C

QUESTION 15

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

Correct Answer: D

Latest 300-720 Dumps 300-720 PDF Dumps 300-720 Exam Questions