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.passapply.com/300-720.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

An engineer must limit responses from the gateway that are directed to invalid email addresses. How should the LDAP server be configured to accomplish this goal?

A. Validate the sender email address via an LDAP query during the SMTP conversation.

B. Validate the sender email address via SMTP Call-Ahead to query an external SMTP server.

C. Limit the number of invalid recipients per sender to stop responses after crossing the threshold.

D. Limit the number of invalid responses per recipient to stop responses after crossing the threshold.

Correct Answer: D

QUESTION 2

An organization wants to use its existing Cisco ESA to host a new domain and enforce a separate corporate policy for that domain.

What should be done on the Cisco ESA to achieve this?

A. Use the smtproutes command to configure a SMTP route for the new domain.

B. Use the deliveryconfig command to configure mail delivery for the new domain.

C. Use the dsestconf command to add a separate destination for the new domain.

D. Use the altrchost command to add a separate gateway for the new domain.

Correct Answer: A

QUESTION 3

Refer to the exhibit.

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

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 4

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

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

Correct Answer: B

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_010010.html

QUESTION 5

Which global setting is configured under Cisco ESA Scan Behavior?

A. minimum attachment size to scan

B. attachment scanning timeout

C. actions for unscannable messages due to attachment type

D. minimum depth of attachment recursion to scan

Correct Answer: B

Reference: https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scan-behavior-impact-on-av/td-p/3923243

QUESTION 6

Which component must be added to the content filter to trigger on failed SPF Verification or DKIM Authentication verdicts?

A. status

B. response

C. parameter

D. condition

Correct Answer: D

QUESTION 7

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

A. 20 MB

B. 25 MB

C. 15 MB

D. 30 MB

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117972-technote-esa-00.html

---

QUESTION 8

A network administrator enabled McAfee antivirus scanning on a Cisco ESA and configured the virus scanning action of "scan for viruses only." If the scanner finds a virus in an attachment for an incoming email, what action will be applied to this message?

A. The attachment is dropped and replaced with a "Removed Attachment" file.

B. The email and attachment are forwarded to the network administrator.

C. The system will attempt to repair the attachment.

D. No repair is attempted, and the attachment is either dropped or delivered.

Correct Answer: D

QUESTION 9

Which feature must be enabled first when URL logging is configured on a Cisco ESA?

A. antivirus

B. antispam

C. senderbase reputation filter

D. virus outbreak filter

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html#:~:text=In%20order%20to%20implement%20URL,CLI%20by%20the%20ESA%20administrator.

QUESTION 10

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 11

Which attack is mitigated by using Bounce Verification?

A. spoof

B. denial of service

C. eavesdropping

D. smurf

Correct Answer: B

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

---

QUESTION 12

What is a valid content filter action?

A. decrypt on delivery

B. quarantine

C. skip antispam

D. archive

Correct Answer: B

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_01010.html#con_1158022

QUESTION 13

Which type of query must be configured when setting up the Spam Quarantine while merging notifications?

A. Spam Quarantine Alias Routing Query

B. Spam Quarantine Alias Consolidation Query

C. Spam Quarantine Alias Authentication Query

D. Spam Quarantine Alias Masquerading Query

Correct Answer: B

QUESTION 14

The CEO sent an email indicating that all emails containing a string of 123ABCDEFGHJ cannot be delivered and must be sent into quarantine for further inspection. Given the requirement, which regular expression should be used to match on that criteria?

A. \d{3}[A?]{9}

B. {3}\d{9}[A?]

C. \w{3}[A?]{9}

D. \\D{3}[A?]{9}

Correct Answer: B

QUESTION 15

What is a category for classifying graymail?

A. Priority

B. Marketing

C. Malicious

D. Spam

Correct Answer: B