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 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

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 3

An administrator manipulated the subnet mask but was still unable to access the user interface. How must the administrator access the appliance to perform the initial configuration?

A. Use the data 2 port.

B. Use the serial or console port.

C. Use the data 1 port.

D. Use the management port.

Correct Answer: B

QUESTION 4

A recent engine update was pulled down for graymail and has caused the service to start crashing. It is critical to fix this as quickly as possible. What must be done to address this issue?

A. Roll back to a previous version of the engine from the Services Overview page.

B. Roll back to a previous version of the engine from the System Health page.

C. Download another update from the IMS and Graymail page.

D. Download another update from the Service Updates page.

Correct Answer: A

Reference: 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_11_1_chapter_0100010.html#task_9F07A032042F48C6AEDB69D325CD3C5F

QUESTION 5

What is a category for classifying graymail?

A. Priority

B. Marketing

C. Malicious

D. Spam

Correct Answer: B

QUESTION 6

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

A. The default engine scans for viruses first and the McAfee engine scans for viruses second.

B. The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.

C. The McAfee engine scans for viruses first and the default engine scans for viruses second.

D. The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.

Correct Answer: C

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.

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_01011.html

QUESTION 7

What is the purpose of checking the CRL during SMTP authentication on a Cisco ESA?

A. Check if the certificate is not revoked.

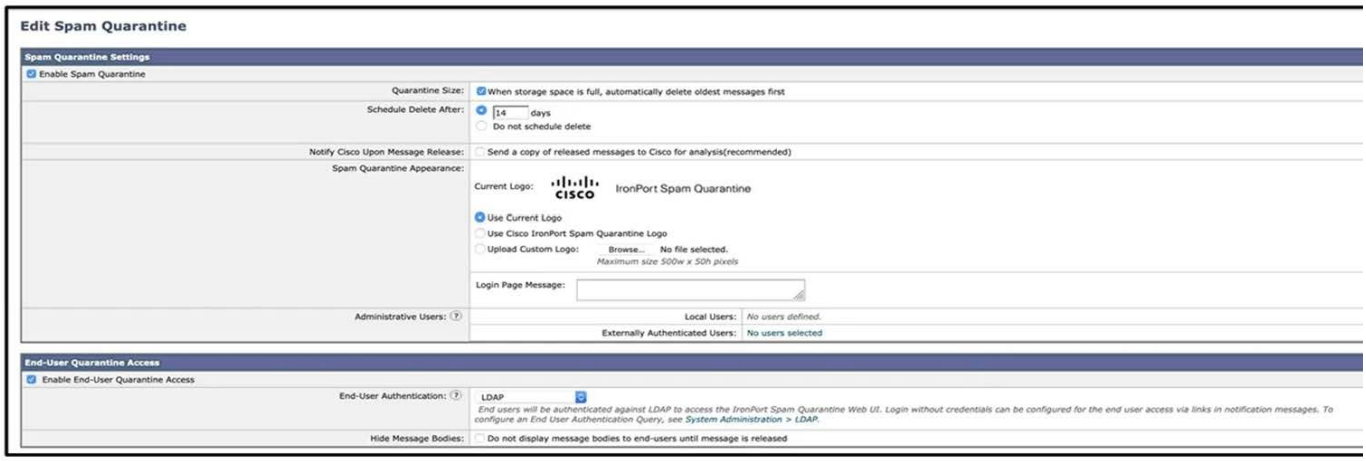
B. Confirm that corresponding CA is present.

C. Verify the common name matches user ID.

D. Validate the date to check if the certificate is still valid.

Correct Answer: A

QUESTION 8



Refer to the exhibits. What must be done to enforce end user authentication before accessing quarantine?

A. Enable SPAM notification and use LDAP for authentication.

B. Enable SPAM Quarantine Notification and add the %quarantine_url% variable.

C. Change the end user quarantine access from None authentication to SAAS.

D. Change the end user quarantine access setting from None authentication to Mailbox.

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure-esa-00.html#anc7

QUESTION 9

A Cisco ESA administrator recently enabled the Outbreak Filters Global Service Setting to detect Viral as well as Non-Viral threat detection, with no detection of Non-Viral threats after 24 hours of monitoring Outbreak Filters. What is the reason that Non-Viral threat detection is not detecting any positive verdicts?

A. The Outbreak Filters option Graymail Header must be enabled.

B. The Outbreak Filters option URL Rewriting must be enabled.

C. Non-Viral threat detection requires AntiSpam or Intelligent Multi-Scan enablement to properly function.

D. Non-Viral threat detection requires AntiVirus or AMP enablement to properly function.

Correct Answer: C

QUESTION 10

A network engineer must tighten up the SPAM control policy of an organization due to a recent SPAM attack. In which scenario does enabling regional scanning improve security for this organization?

A. when most of the received email originates outside of the U.S.

B. when most of the received email originates from a specific region

C. when most of the received spam originates outside of the U.S.

D. when most of the received spam comes from a specific country

Correct Answer: D

QUESTION 11

To comply with a recent audit, an engineer must configure anti-virus message handling options on the incoming mail policies to attach warnings to the subject of an email. What should be configured to meet this requirement for known viral emails?

A. Virus Infected Messages

B. Unscannable Messages

C. Encrypted Messages

D. Positively Identified Messages

Correct Answer: C

QUESTION 12

A network administrator is modifying an outgoing mail policy to enable domain protection for the organization. A DNS entry is created that has the public key. Which two headers will be used as matching criteria in the outgoing mail policy? (Choose two.)

A. message-ID

B. sender

C. URL reputation

D. from

E. mail-from

Correct Answer: BD

QUESTION 13

Which two Cisco ESA features are used to control email delivery based on the sender? (Choose two.)

A. incoming mail policies

B. spam quarantine

C. outbreak filter

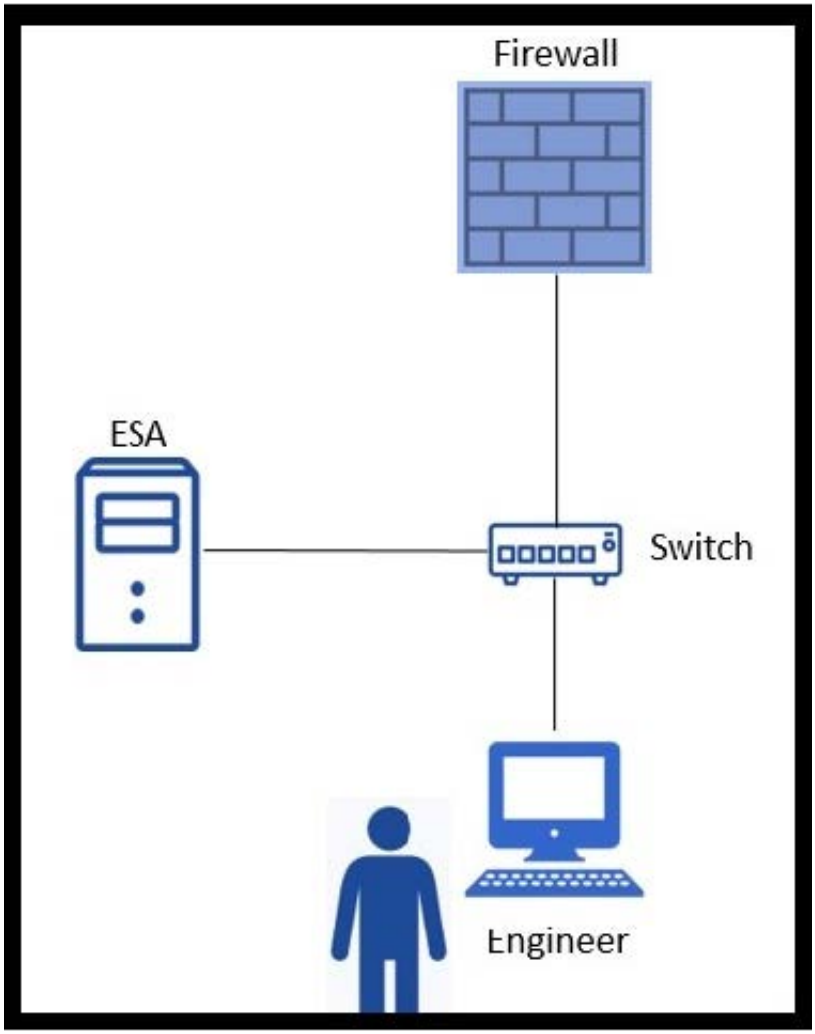
D. safelists

E. blocklists

Correct Answer: DE

QUESTION 14

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?

A. Telnet

B. HTTPS

C. Ethernet

D. serial

Correct Answer: D

QUESTION 15

An administrator has created a content filter to quarantine all messages that result in an SPF hardfail to review the messages and determine whether a trusted partner has accidentally misconfigured the DNS settings. The administrator sets the policy quarantine to release the messages after 24 hours, allowing time to review while not interrupting business.

Which additional option should be used to help the end users be aware of the elevated risk of interacting with these messages?

A. Notify Recipient

B. Strip Attachments

C. Notify Sender

D. Modify Subject

Correct Answer: D