

100% Money Back
Guarantee

Vendor:Cisco

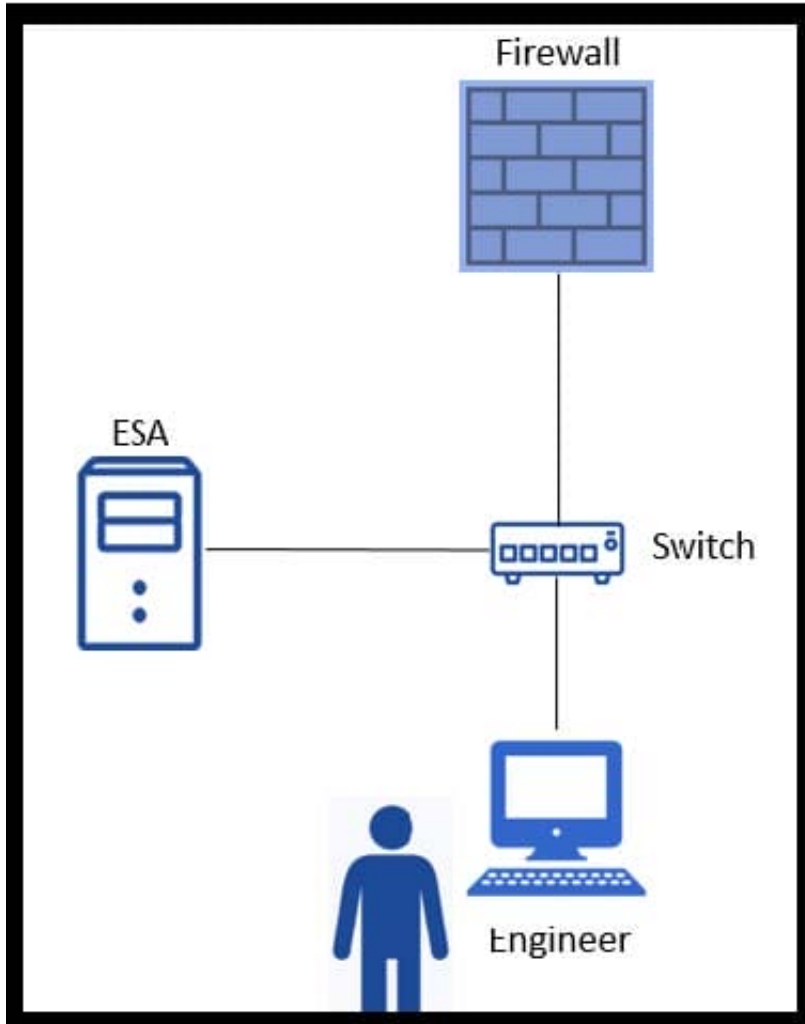
Exam Code:300-720

Exam Name:Securing Email with Cisco Email Security
Appliance (SESA)

Version:Demo

QUESTION 1

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 2

DRAG DROP

An Encryption Profile has been set up on the Cisco ESA.

Drag and drop the steps from the left for creating an outgoing content filter to encrypt emails that contains the subject "Secure:" into the correct order on the right.

Select and Place:

Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).	step 1
Submit and commit the changes.	step 2
Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.	step 3
Choose the outgoing content filters.	step 4

Correct Answer:

	Choose the outgoing content filters.
	Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).
	Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.
	Submit and commit the changes.

Reference: <https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/td-p/2441383>

QUESTION 3

An administrator needs to configure a Cisco ESA to verify that a specific mail server is authorized to send emails for a domain. To reduce overhead, the administrator does not want SSL type encryption or decryption to be used in this process. What must be configured on the Cisco ESA to meet this requirement?

- A. DomainKeys Identified Mail
- B. PKI signing keys
- C. Asymmetric keys
- D. Sender Policy Framework

Correct Answer: D

QUESTION 4

A network administrator notices that there are a high number of queries to the LDAP server. The mail logs show an entry "550 Too many invalid recipients | Connection closed by foreign host." Which feature must be used to address this?

- A. DHAP
- B. SBRS
- C. LDAP
- D. SMTP

Correct Answer: D

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_12_0_chapter_011010.html

QUESTION 5

An engineer is configuring a Cisco ESA for the first time and needs to ensure that any email traffic coming from the internal SMTP servers is relayed out through the Cisco ESA and is tied to the Outgoing Mail Policies. Which Mail Flow Policy setting should be modified to accomplish this goal?

- A. Exception List
- B. Connection Behavior
- C. Bounce Detection Signing
- D. Reverse Connection Verification

Correct Answer: B

Reference: <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html>

QUESTION 6

Which antispam feature is utilized to give end users control to allow emails that are spam to be delivered to their inbox, overriding any spam verdict and action on the Cisco ESA?

- A. end user allow list
- B. end user spam quarantine access
- C. end user passthrough list
- D. end user safelist

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide

QUESTION 7

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>

QUESTION 8

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 9

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 10

An administrator is managing multiple Cisco ESA devices and wants to view the quarantine emails from all devices in a central location. How is this accomplished?

- A. Disable the VOF feature before sending SPAM to the external quarantine.
- B. Configure a mail policy to determine whether the message is sent to the local or external quarantine.
- C. Disable the local quarantine before sending SPAM to the external quarantine.
- D. Configure a user policy to determine whether the message is sent to the local or external quarantine.

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_12_0_chapter_0100000.html#task_1749146

QUESTION 11

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

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

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-0/user_guide/b_SMA_Admin_Guide/b_SMA_Admin_Guide_chapter_010101.html

QUESTION 12

Refer to the exhibit.

```

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 marketing team in the inbound table
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/524208) for scanning by Outbreak Filters
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/2097152) for scanning by CASE
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: GRAYMAIL negative
Tue Aug 13 16:55:52 2019 Info: MID 379133 attachment 'ds_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			
Fingerprint/MIME	Type	Edit	Delete
Fingerprint	Image	Edit...	
Fingerprint	Media	Edit...	
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	

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

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

Correct Answer: A