Vendor: Cisco

Exam Code: 300-720

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

Version: DEMO

QUESTION 1
Which two are configured in the DMARC verification profile? (Choose two.)

A. name of the verification profile
B. minimum number of signatures to verify
C. ESA listeners to use the verification profile
D. message action into an incoming or outgoing content filter
E. message action to take when the policy is reject/quarantine

Answer: AE
Explanation:
A DMARC verification profile consists of the following information:
A name for the verification profile.
Message action to take when the policy in the DMARC record is reject.
Message action to take when the policy in the DMARC record is quarantine.
Message action in case of a temporary failure.
Message action in case of a permanent failure.

QUESTION 2
What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

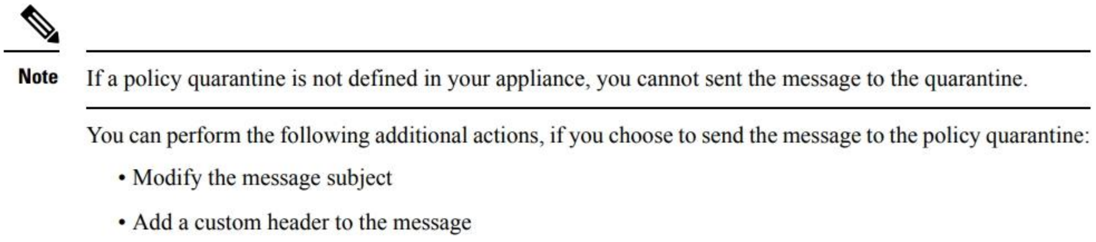
A. 83
B. 82
C. 443
D. 80

Answer: A
Explanation:
In the Spam Quarantine section, configure settings for access to the spam quarantine:
By default, HTTP uses port 82 and HTTPS uses port 83.

QUESTION 3
Which scenario prevents a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA?

A. A policy quarantine is missing.
B. More than one email pipeline is defined.
C. The "modify the message subject" is already set.
D. The "add custom header" action is performed first.

Answer: A
Explanation:



Note If a policy quarantine is not defined in your appliance, you cannot sent the message to the quarantine.

You can perform the following additional actions, if you choose to send the message to the policy quarantine:

- Modify the message subject
- Add a custom header to the message

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.320

QUESTION 4
When email authentication is configured on Cisco ESA, which two key types should be selected on the signing profile? (Choose two.)

A. DKIM
B. Public Keys
C. Domain Keys
D. Symmetric Keys
E. Private Keys

Answer: AC
Explanation:
DomainKeys and DKIM signing works like this: a domain owner generates two keys - a public key stored in the public DNS (a DNS TXT record associated with that domain) and a private key that is stored on the appliance is used to sign mail that is sent (mail that originates) from that domain.
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa-configure-dkim-signing.html

QUESTION 5
Which setting affects the aggressiveness of spam detection?

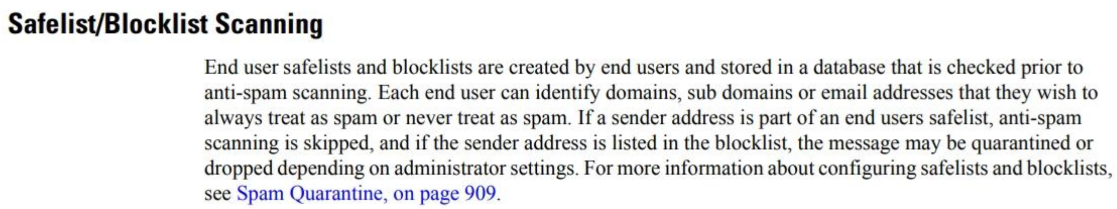
A. protection level
B. spam threshold
C. spam timeout
D. maximum depth of recursion scan

Answer: B
Explanation:
Apply more aggressive spam thresholds if false-positives are less of a concern than missed spam:
- Reduce the Positive Spam Threshold to 80 (default is 90) if false-positives are not a concern at the 'certain' threshold.
- Reduce Suspected Spam Threshold to 40 (default is 50) if false-positives are not a concern at the 'suspect' threshold.

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

Answer: D
Explanation:



Safelist/Blocklist Scanning

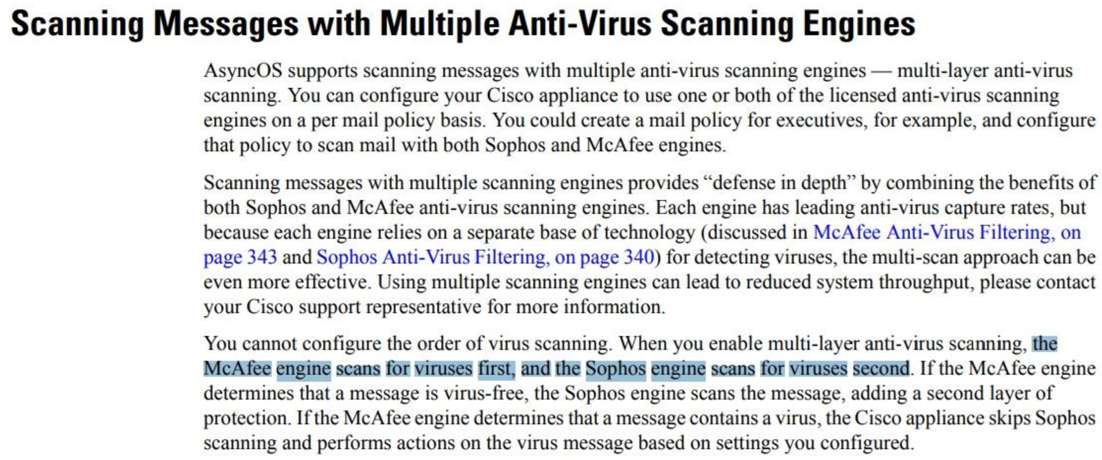
End user safelists and blocklists are created by end users and stored in a database that is checked prior to anti-spam scanning. Each end user can identify domains, sub domains or email addresses that they wish to always treat as spam or never treat as spam. If a sender address is part of an end users safelist, anti-spam scanning is skipped, and if the sender address is listed in the blocklist, the message may be quarantined or dropped depending on administrator settings. For more information about configuring safelists and blocklists, see Spam Quarantine, on page 909.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.129

QUESTION 7
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.

Answer: D
Explanation:



Scanning Messages with Multiple Anti-Virus Scanning Engines

AsyncOS supports scanning messages with multiple anti-virus scanning engines — multi-layer anti-virus scanning. You can configure your Cisco appliance to use one or both of the licensed anti-virus scanning engines on a per mail policy basis. You could create a mail policy for executives, for example, and configure that policy to scan mail with both Sophos and McAfee engines.

Scanning messages with multiple scanning engines provides "defense in depth" by combining the benefits of both Sophos and McAfee anti-virus scanning engines. Each engine has leading anti-virus capture rates, but because each engine relies on a separate base of technology (discussed in McAfee Anti-Virus Filtering, on page 343 and Sophos Anti-Virus Filtering, on page 340) for detecting viruses, the multi-scan approach can be even more effective. Using multiple scanning engines can lead to reduced system throughput, please contact your Cisco support representative for more information.

You cannot configure the order of virus scanning. When you enable multi-layer anti-virus scanning, the McAfee engine scans for viruses first, and the Sophos engine scans for viruses second. If the McAfee engine determines that a message is virus-free, the Sophos engine scans the message, adding a second layer of protection. If the McAfee engine determines that a message contains a virus, the Cisco appliance skips Sophos scanning and performs actions on the virus message based on settings you configured.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.402

QUESTION 8
Which action is a valid fallback when a client certificate is unavailable during SMTP authentication on Cisco ESA?

A. LDAP Query
B. SMTP AUTH
C. SMTP TLS
D. LDAP BIND

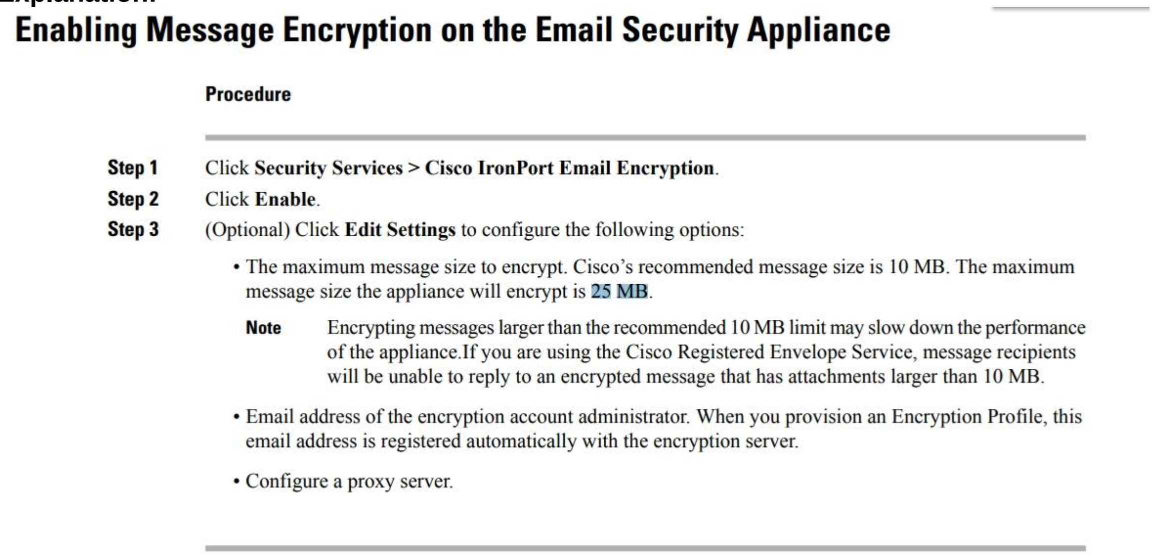
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011011.html

The certificate-based SMTP authentication profile allows the appliance to authenticate an SMTP connection over TLS using a client certificate. When creating the profile, you select the Certificate Authentication LDAP query to use for verifying the certificate. You can also specify whether the appliance falls back to the SMTP AUTH command to authenticate the user if a client certificate is not available.

QUESTION 9
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

Answer: B
Explanation:



Enabling Message Encryption on the Email Security Appliance

Procedure

Step 1 Click **Security Services > Cisco IronPort Email Encryption**.

Step 2 Click **Enable**.

Step 3 (Optional) Click **Edit Settings** to configure the following options:

- The maximum message size to encrypt. Cisco's recommended message size is 10 MB. The maximum message size the appliance will encrypt is 25 MB.

  Note Encrypting messages larger than the recommended 10 MB limit may slow down the performance of the appliance.If you are using the Cisco Registered Envelope Service, message recipients will be unable to reply to an encrypted message that has attachments larger than 10 MB.

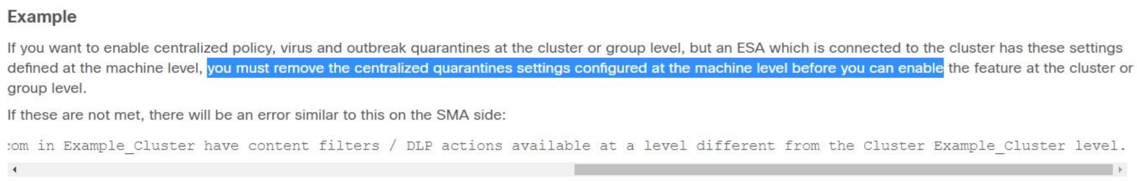
- Email address of the encryption account administrator. When you provision an Encryption Profile, this email address is registered automatically with the encryption server.
- Configure a proxy server.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.580

QUESTION 10
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.

Answer: A
Explanation:



Example

If you want to enable centralized policy, virus and outbreak quarantines at the cluster or group level, but an ESA which is connected to the cluster has these settings defined at the machine level, you must remove the centralized quarantines settings configured at the machine level before you can enable the feature at the cluster or group level.

If these are not met, there will be an error similar to this on the SMA side:

```
:om in Example_Cluster have content filters / DLP actions available at a level different from the Cluster Example_Cluster level.
```

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200083-Requirements-for-the-PVO-Migration-Wizar.html

QUESTION 11
Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?

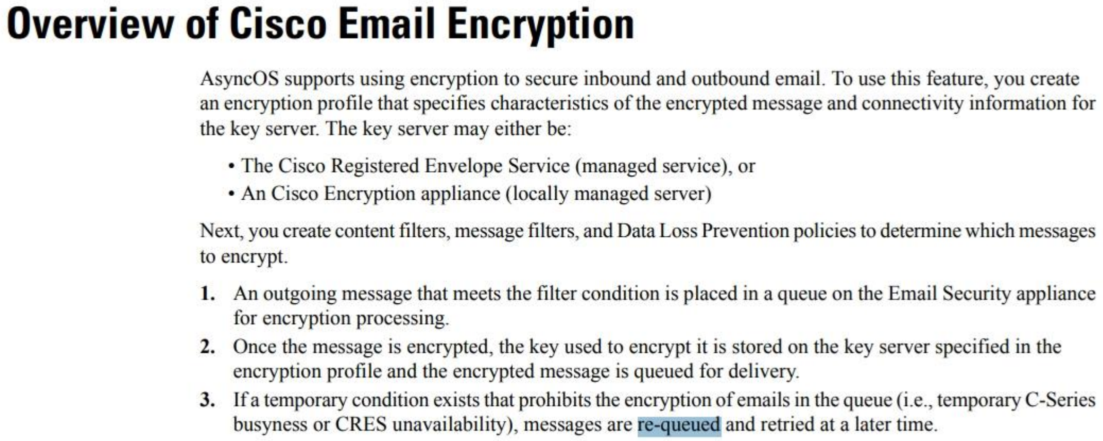
A. Set up the interface group with the flag.
B. Issue the altsrchost command.
C. Map the envelope sender address to the host.
D. Apply a filter on the message.

Answer: D
Explanation:
Using message filters, you can set up specific filters to deliver flagged messages using a specific host IP interface (Virtual Gateway address) or interface group. See Alter Source Host (Virtual Gateway address) Action. (This method is more flexible and powerful than the one above.)

QUESTION 12
Email encryption is configured on a Cisco ESA that uses CRES.
Which action is taken on a message when CRES is unavailable?

A. It is requeued.
B. It is sent in clear text.
C. It is dropped and an error message is sent to the sender.
D. It is encrypted by a Cisco encryption appliance.

Answer: A
Explanation:



Overview of Cisco Email Encryption

AsyncOS supports using encryption to secure inbound and outbound email. To use this feature, you create an encryption profile that specifies characteristics of the encrypted message and connectivity information for the key server. The key server may either be:

- The Cisco Registered Envelope Service (managed service), or
- An Cisco Encryption appliance (locally managed server)

Next, you create content filters, message filters, and Data Loss Prevention policies to determine which messages to encrypt.

1. An outgoing message that meets the filter condition is placed in a queue on the Email Security appliance for encryption processing.
2. Once the message is encrypted, the key used to encrypt it is stored on the key server specified in the encryption profile and the encrypted message is queued for delivery.
3. If a temporary condition exists that prohibits the encryption of emails in the queue (i.e., temporary C-Series busyness or CRES unavailability), messages are re-queued and retried at a later time.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.577