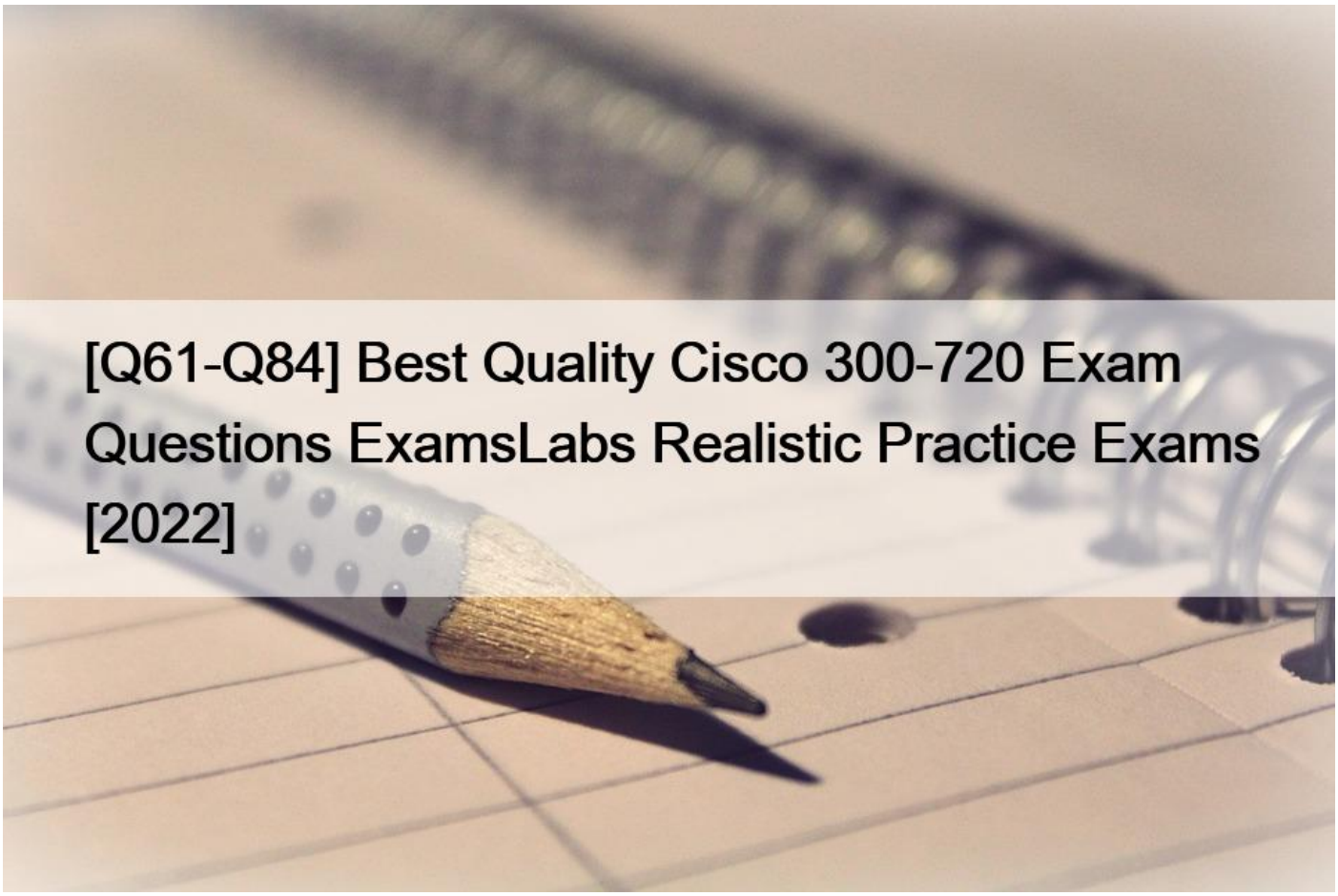
[Q61-Q84 Best Quality Cisco 300-720 Exam Questions ExamsLabs Realistic Practice Exams [2022



Best Quality Cisco 300-720 Exam Questions ExamsLabs Realistic Practice Exams [2022]
Critical Information To Securing Email with Cisco Email Security Appliance Pass the First Time

What is the amount for Cisco 300-720 Exam - The price of the Cisco 300-720 Exam is $300 USD.

Cisco 300-720 Exam Syllabus Topics:

Topic	Details
Topic 1	- Describe Centralized Services On A Cisco Content Sma- System Quarantines And Delivery Methods
Topic 2	- Configure File Reputation Filtering And File Analysis Features- Implement Malicious Or Undesirable Urls Protection
Topic 3	- Configure And Verify Ldap Servers And Queries- Cisco Email Security Appliance Administration
Topic 4	- Configure Quarantine (Spam, Policy, Virus, And Outbreak)- Incoming And Outgoing Messages
Topic 5	- Manage Certificate Authorities- Configure Virtual Gateways- Configure Email Encryption
Topic 6	- Describe S- Mime Security Services And Communication Encryption With Other Mtas
Topic 7	- Create Text Resources Such As Content Dictionaries, Disclaimers, And Templates- Hardware Performance Specifications
Topic 8	- Configure Data Loss Prevention (Dlp)- Understand Smtp Functionality- Configure Dmarc Verification

QUESTION 61

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?
* Exception List
* Connection Behavior
* Bounce Detection Signing
* Reverse Connection Verification

QUESTION 62

What are organizations trying to address when implementing a SPAM quarantine?
* true positives
* false negatives
* false positives
* true negatives

QUESTION 63

Which type of attack is prevented by configuring file reputation filtering and file analysis features?
* denial of service
* zero-day
* backscatter
* phishing

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_010000.html#con_1809885

QUESTION 64

Which two components form the graymail management solution in Cisco ESA? (Choose two.)
* cloud-based unsubscribe service
* uniform unsubscription management interface for end users
* secure subscribe option for end users
* integrated graymail scanning engine
* improved mail efficacy

QUESTION 65

What are two primary components of content filters? (Choose two.)
* conditions
* subject
* content
* actions
* policies

Explanation/Reference:

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_01010.pdf

QUESTION 66

Which two action types are performed by Cisco ESA message filters? (Choose two.)
* non-final actions
* filter actions
* discard actions
* final actions
* quarantine actions

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_chapter_01000.html

QUESTION 67

Which global setting is configured under Cisco ESA Scan Behavior?
* minimum attachment size to scan
* attachment scanning timeout
* actions for unscannable messages due to attachment type
* minimum depth of attachment recursion to scan

Reference:

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

QUESTION 68

Which two components must be configured to perform DLP scanning? (Choose two.)
* Add a DLP policy on the Incoming Mail Policy.
* Add a DLP policy to the DLP Policy Manager.
* Enable a DLP policy on the Outgoing Mail Policy.
* Enable a DLP policy on the DLP Policy Customizations.
* Add a DLP policy to the Outgoing Content Filter.

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_chapter_010001.html

QUESTION 69

An engineer is tasked with reviewing mail logs to confirm that messages sent from domain abc.com are passing SPF verification and being accepted by the Cisco ESA. The engineer notices that SPF verification is not being performed and that SPF is not being referenced in the logs for messages sent from domain abc.com.

Why is the verification not working properly?
* SPF verification is disabled in the Recipient Access Table.
* SPF verification is disabled on the Mail Flow Policy.
* The SPF conformance level is set to SIDF compatible on the Mail Flow Policy.

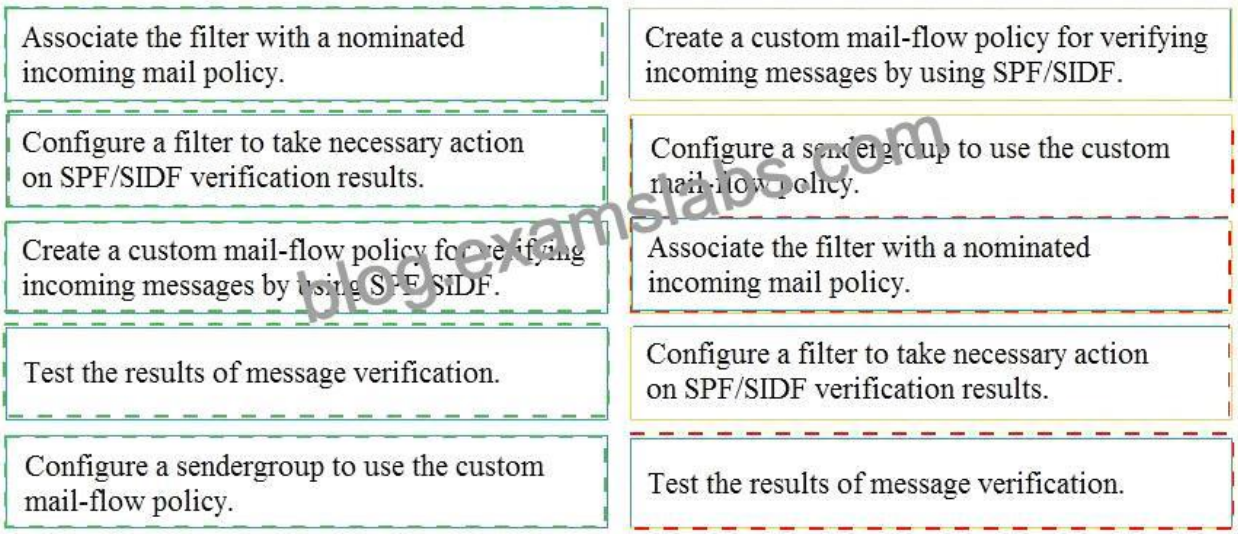
* An SPF verification Content Filter has not been created.

QUESTION 70

Which two query types are available when an LDAP profile is configured? (Choose two.)
* proxy consolidation
* user
* recursive
* group
* routing

QUESTION 71

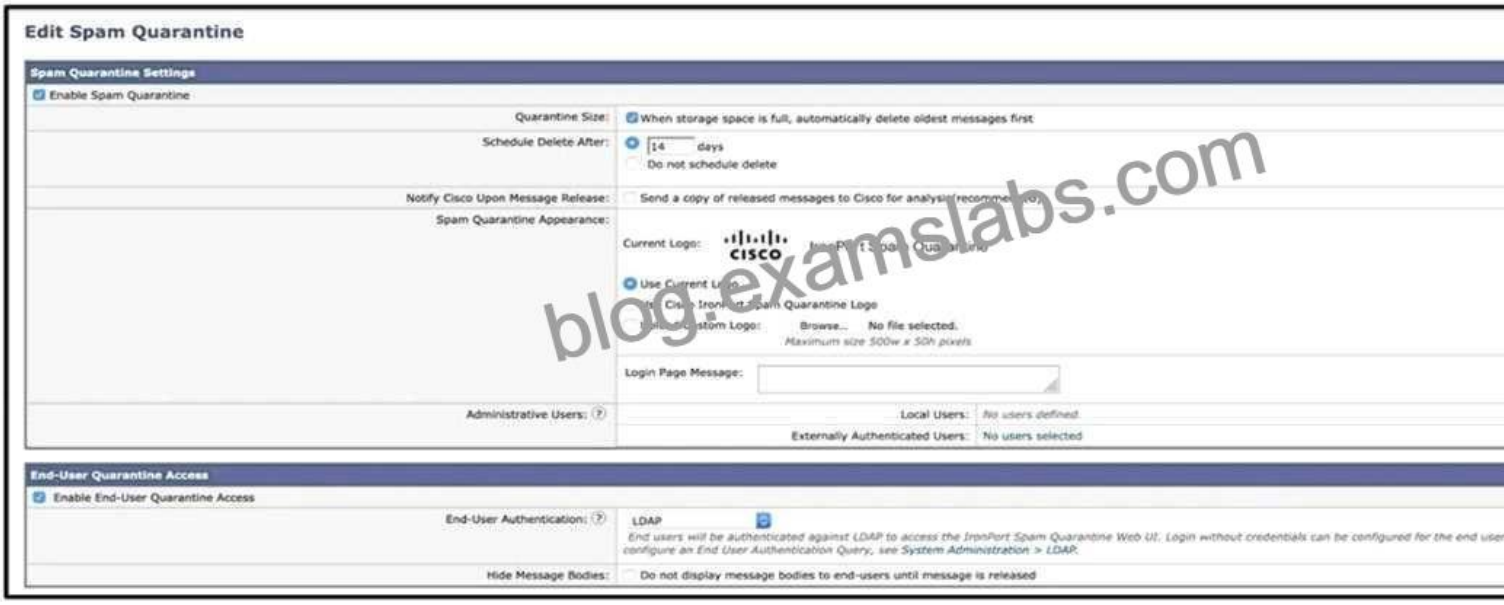
Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.

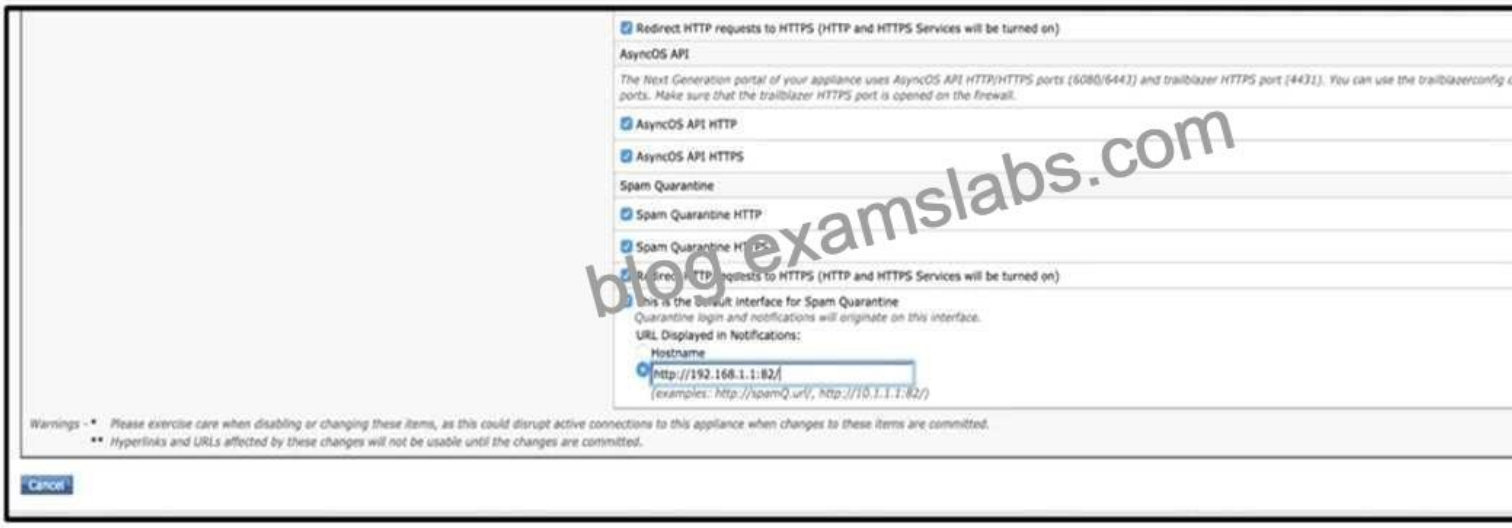


Associate the filter with a nominated incoming mail policy.	Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.
Configure a filter to take necessary action on SPF/SIDF verification results.	Configure a sendergroup to use the custom mail-flow policy.
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	Associate the filter with a nominated incoming mail policy.
Test the results of message verification.	Configure a filter to take necessary action on SPF/SIDF verification results.
Configure a sendergroup to use the custom mail-flow policy.	Test the results of message verification.

QUESTION 72

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





* Enable SPAM notification and use LDAP for authentication.
* Enable SPAM Quarantine Notification and add the %quarantine_url% variable.
* Change the end user quarantine access from None authentication to SAAS.
* Change the end user quarantine access setting from None authentication to Mailbox.

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

QUESTION 73

Which two steps configure Forged Email Detection? (Choose two.)
* Configure a content dictionary with executive email addresses.
* Configure a filter to use the Forged Email Detection rule and dictionary.
* Configure a filter to check the Header From value against the Forged Email Detection dictionary.
* Enable Forged Email Detection on the Security Services page.
* Configure a content dictionary with friendly names.

QUESTION 74

Which two factors must be considered when message filter processing is configured? (Choose two.)
* message-filter order
* lateral processing
* structure of the combined packet
* mail policies
* MIME structure of the message

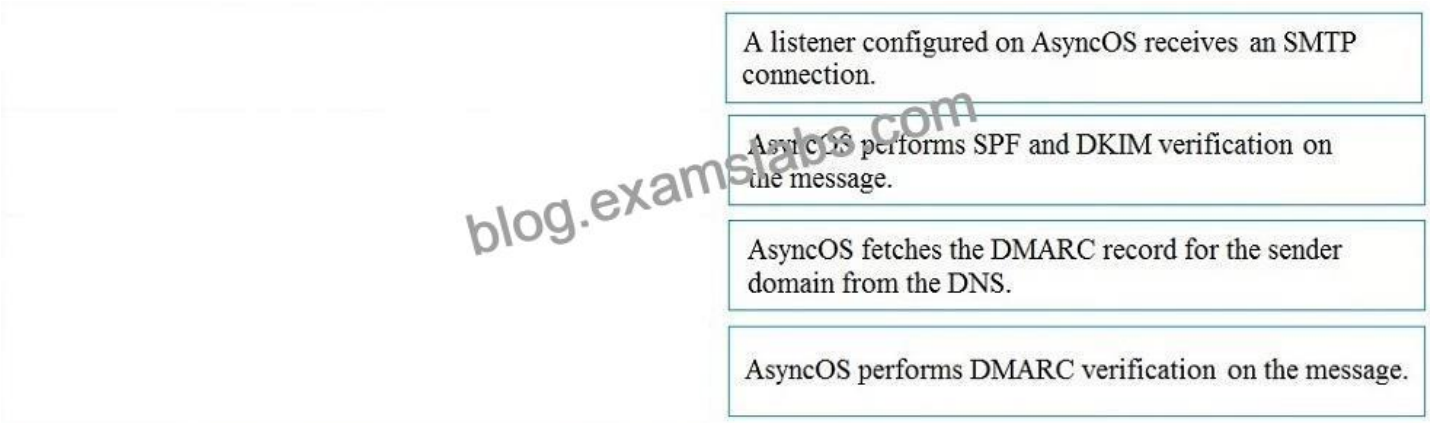
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01000.html

QUESTION 75

Drag and Drop Question

Drag and drop the AsyncOS methods for performing DMARC verification from the left into the correct order on the right.

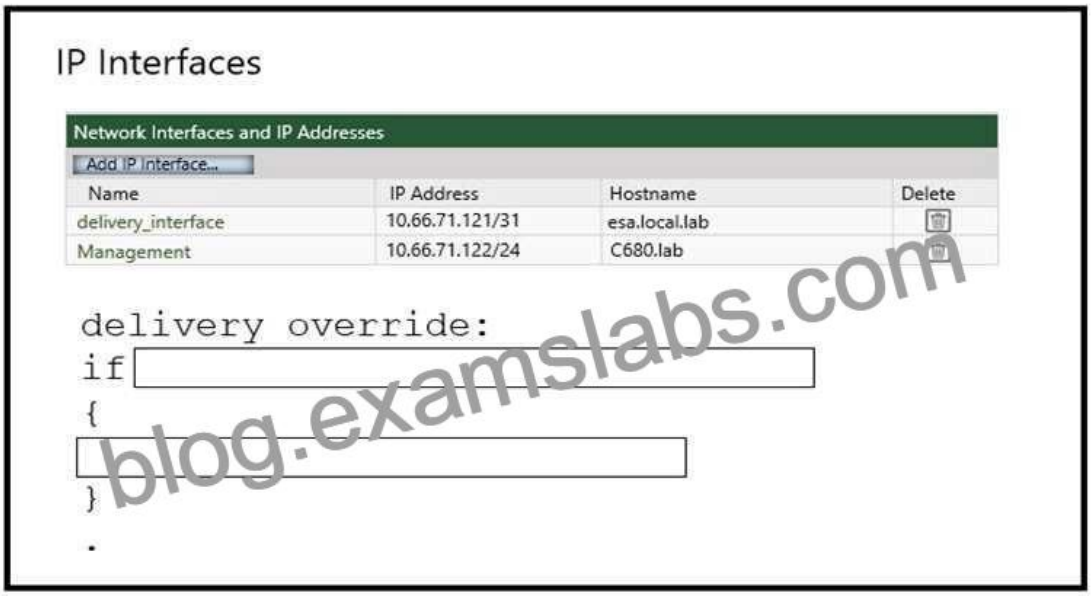
AsyncOS performs DMARC verification on the message.	step 1
A listener configured on AsyncOS receives an SMTP connection.	step 2
AsyncOS performs SPF and DKIM verification on the message.	step 3
AsyncOS fetches the DMARC record for the sender domain from the DNS.	step 4



QUESTION 76

Drag and Drop Question

An administrator must ensure that emails sent from cisco_123@externally.com are routed through an alternate virtual gateway. Drag and drop the snippet from the bottom onto the blank in the graphic to finish the message filter syntax. Not all snippets are used.




```
Envelope-sender ==“cisco_123@externally.com”
mail-from ==“cisco_123@externally.com”
Sender ==“cisco_123@externally.com
delivery-int(“delivery_interface”);
alt-src-host(“delivery_interface”);
```


```
Envelope-sender ==“cisco_123@externally.com”

Sender ==“cisco_123@externally.com

alt-src-host(“delivery_interface”);
```

QUESTION 77

Which two certificate authority lists are available in Cisco ESA? (Choose two.)
* default
* system
* user
* custom
* demo

QUESTION 78

What must be configured to allow the Cisco ESA to encrypt an email using the Cisco Registered Envelope Service?
* provisioned email encryption profile
* message encryption from a content filter that select “Message Encryption” over TLS
* message encryption from the mail flow policies with “CRES” selected
* content filter to forward the email to the Cisco Registered Envelope server

QUESTION 79

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?
* end user allow list
* end user spam quarantine access
* end user passthrough list
* end user safelist

QUESTION 80

Which two components must be configured to perform DLP scanning? (Choose two.)
* Add a DLP policy on the Incoming Mail Policy.
* Add a DLP policy to the DLP Policy Manager.
* Enable a DLP policy on the Outgoing Mail Policy.
* Enable a DLP policy on the DLP Policy Customizations.
* Add a DLP policy to the Outgoing Content Filter.

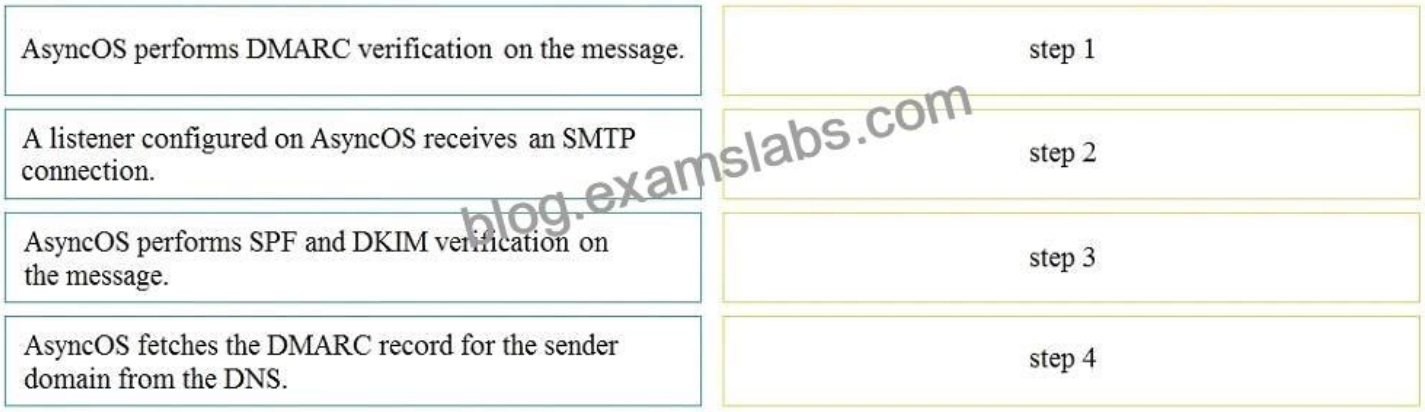
QUESTION 81

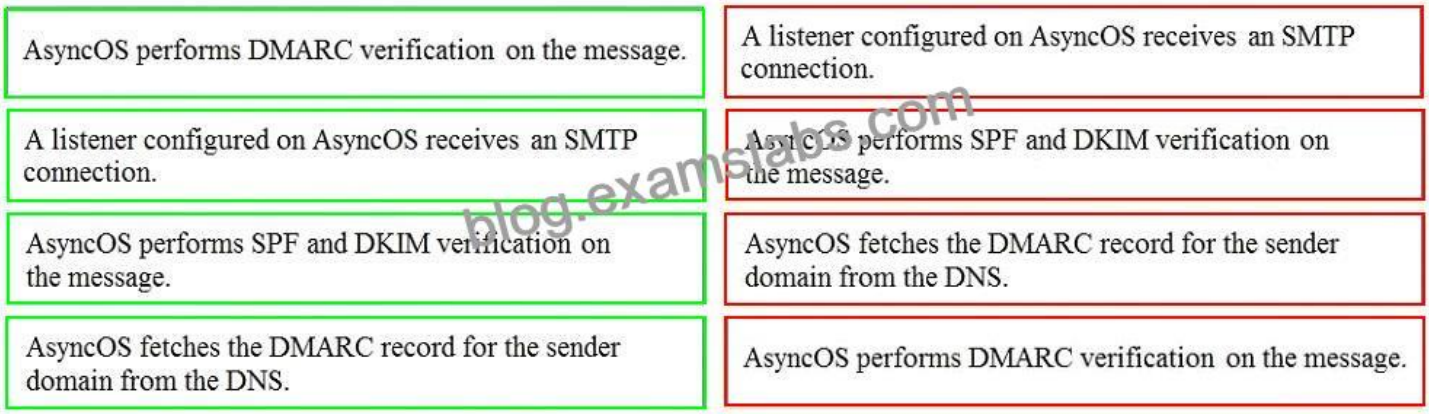
An administrator is trying to enable centralized PVO but receives the error, “Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines configuration as esa1 in Cluster has content filters / DLP actions available at a level different from the cluster level.” What is the cause of this error?
* Content filters are configured at the machine-level on esa1.
* DLP is configured at the cluster-level on esa2.
* DLP is configured at the domain-level on esa1.
* DLP is not configured on host1.

Explanation/Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html

QUESTION 82

Drag and drop the AsyncOS methods for performing DMARC verification from the left into the correct order on the right.





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_010101.html

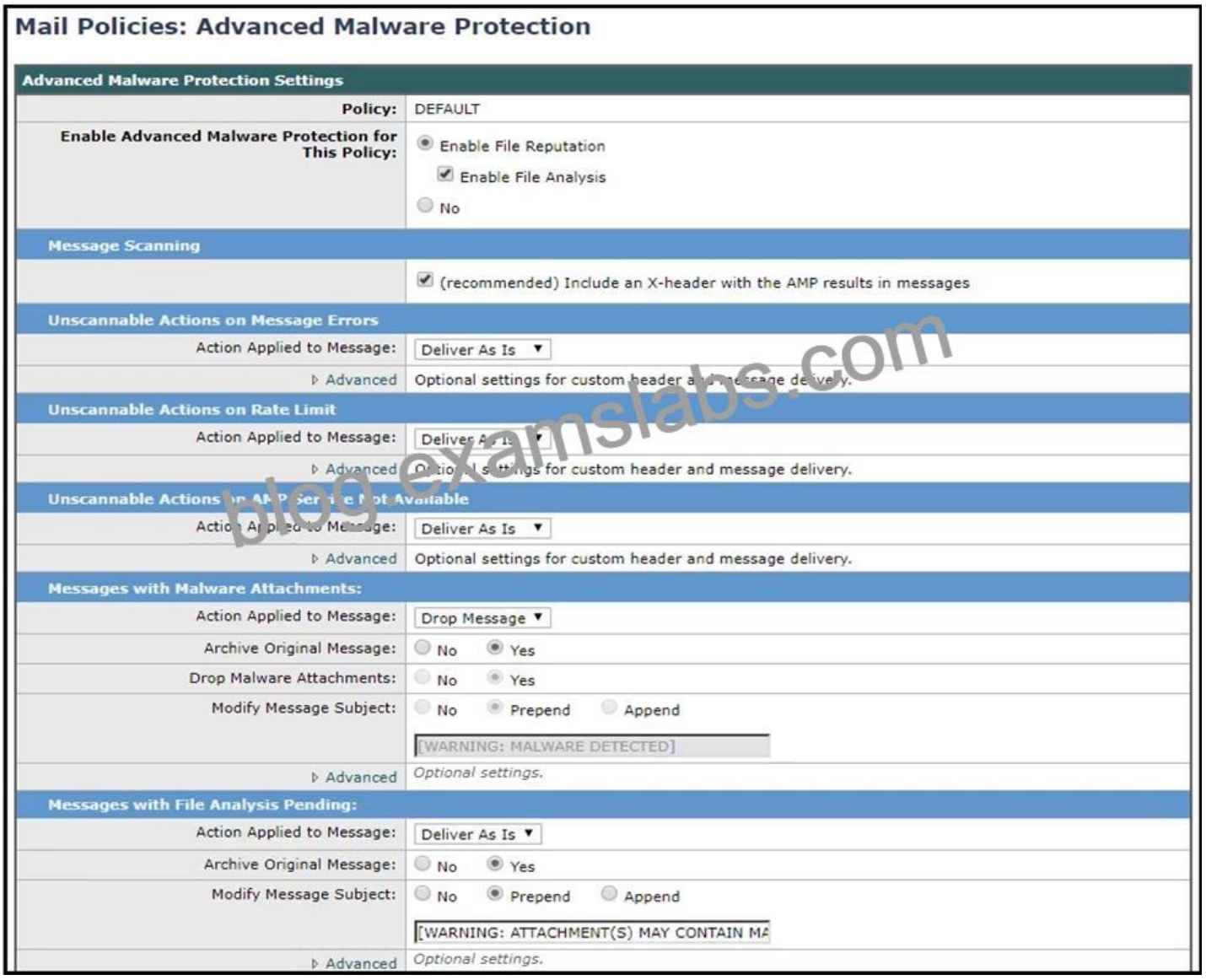
QUESTION 83

A company has deployed a new mandate that requires all emails sent externally from the Sales Department to be scanned by DLP for PCI-DSS compliance. A new DLP policy has been created on the Cisco ESA and needs to be assigned to a mail policy named ‘Sales’ that has yet to be created.

Which mail policy should be created to accomplish this task?

* Outgoing Mail Policy
* Preliminary Mail Policy
* Incoming Mail Flow Policy
* Outgoing Mail Flow Policy

QUESTION 84



Refer to the exhibit. How should this configuration be modified to stop delivering Zero Day malware attacks?

* Change Unscannable Action from Deliver As Is to Quarantine.
* Change File Analysis Pending action from Deliver As Is to Quarantine.
* Configure mailbox auto-remediation.
* Apply Prepend on Modify Message Subject under Malware Attachments.

To get more details visit:

Cisco 300-720 Exam Reference

300-720 EXAM DUMPS WITH GUARANTEED SUCCESS:
https://www.examslabs.com/Cisco/CCNP-Security/best-300-720-exam-dumps.html]