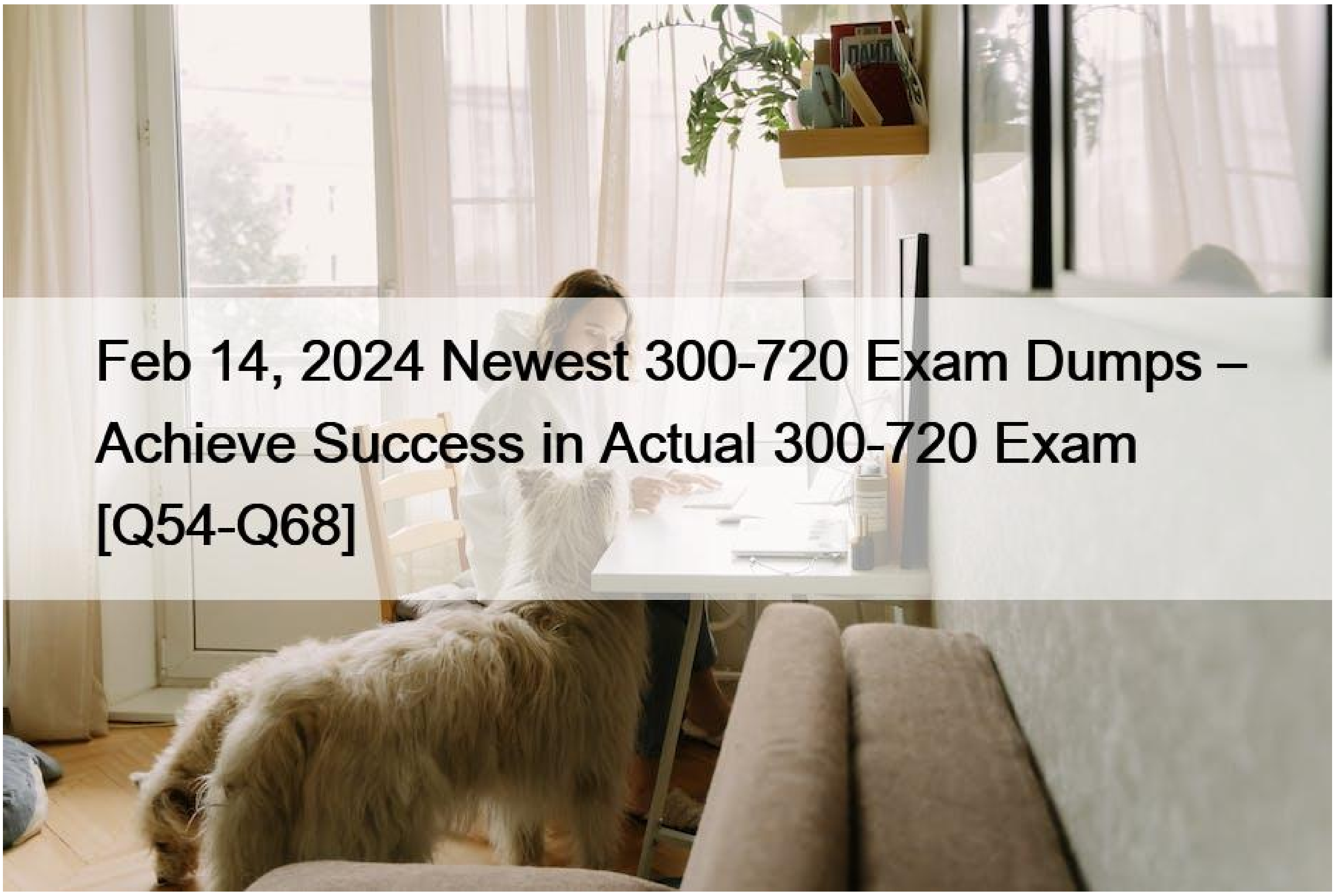
Feb 14, 2024 Newest 300-720 Exam Dumps ? Achieve Success in Actual 300-720 Exam [Q54-Q68


Feb 14, 2024 Newest 300-720 Exam Dumps –
Achieve Success in Actual 300-720 Exam
[Q54-Q68]

Feb 14, 2024 Newest 300-720 Exam Dumps &ndash; Achieve Success in Actual 300-720 Exam
Updated Cisco 300-720 Dumps &ndash; Check Free 300-720 Exam Dumps (2024)

NO.54 How does the graymail safe unsubscribe feature function?
* It strips the malicious content of the URI before unsubscribing.
* It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.
* It checks the URI reputation and category and allows the content filter to take an action on it.
* It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.

Secure unsubscribe option for end users. Mimicking an unsubscribe option is a popular phishing technique. For this reason, the end users are generally wary of clicking unknown unsubscribe links. For such scenarios, the cloud-based Unsubscribe Service extracts the original unsubscribe URI, checks the reputation of the URI, and then performs the unsubscribe process on behalf of the end user. This protects end users from malicious threats masquerading as unsubscribe links.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2-1/User_Guide/b_ESA_Admin_Guide_14-2-1/b_ESA_Admin_Guide_12_1_chapter_01110.html#id_101033

NO.55 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

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

NO.56 A Cisco ESA administrator has noticed that new messages being sent to the Centralized Policy Quarantine are being released after one hour. Previously, they were being held for a day before being released.

What was configured that caused this to occur?

* The retention period was changed to one hour.
* The threshold settings were set to override the clock settings.
* The retention period was set to default.
* The threshold settings were set to default.

NO.57 Which restriction is in place for end users accessing the spam quarantine on Cisco Secure Email Gateway appliances?

* Access via a link in a notification is mandatory.
* The end user must be assigned to the Guest role
* Direct access via web browser requires authentication.
* Authentication is required when accessing via a link in a notification.

Direct access via web browser requires authentication is the restriction that is in place for end users accessing the spam quarantine on Cisco Secure Email Gateway appliances. Spam quarantine is a feature that allows Cisco ESA to store messages that are suspected to be spam and allow end users or administrators to review them and release or delete them as needed.

End users can access their personal spam quarantine on Cisco ESA either by clicking on a link in a notification email or by entering their email address and password in a web browser. In both cases, authentication is required to ensure security and privacy.

The other options are not valid restrictions that are in place for end users accessing the spam quarantine on Cisco Secure Email Gateway appliances, because they are either not mandatory or not related to authentication.

NO.58 Which two certificate authority lists are available in Cisco ESA? (Choose two.)

* default
* system
* user
* custom
* demo

System: This is the default list of trusted certificate authorities that is provided by Cisco and updated automatically. It contains the certificates of well-known and widely used certificate authorities, such as VeriSign, Thawte, and GoDaddy.

Custom: This is the list of additional certificate authorities that you can add manually or import from a file. It allows you to trust certificates that are issued by your own or third-party certificate authorities that are not included in the system list.

NO.59 Which two action types are performed by Cisco ESA message filters? (Choose two.)

* non-final actions
* filter actions
* discard actions
* final actions

* quarantine actions
Non-final actions are actions that do not terminate the message filter evaluation, such as adding headers, setting variables, logging, etc. Final actions are actions that end the message filter evaluation and determine the fate of the message, such as accept, drop, bounce, quarantine, etc.

NO.60 Which action must be taken before a custom quarantine that is being used can be deleted?
* Delete the quarantine that is assigned to a filter.
* Delete the quarantine that is not assigned to a filter.
* Delete only the unused quarantine.
* Remove the quarantine from the message action of a filter.
Before a custom quarantine that is being used can be deleted, it must be removed from the message action of any filter that is using it on Cisco ESA. Otherwise, an error message will appear stating that the quarantine cannot be deleted because it is in use.

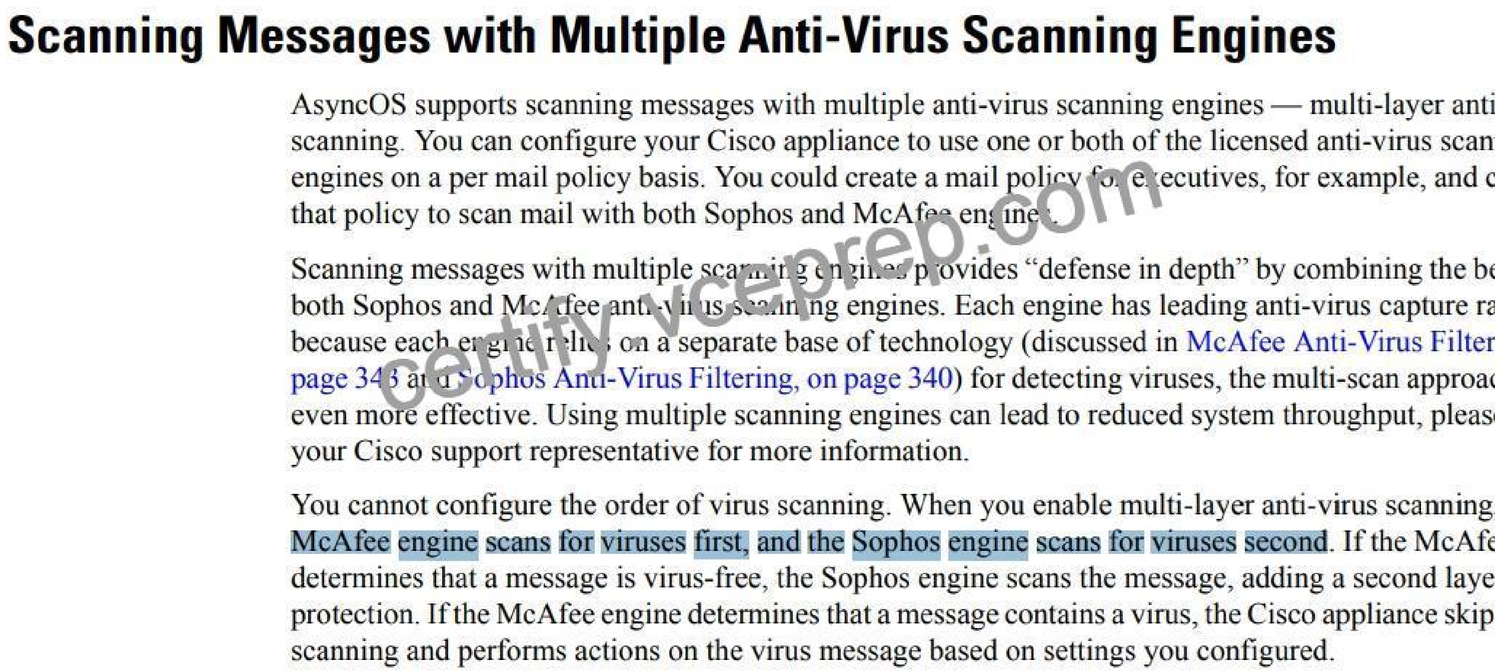
NO.61 A Cisco ESA administrator was notified that a user was not receiving emails from a specific domain. After reviewing the mail logs, the sender had a negative sender-based reputation score.

What should the administrator do to allow inbound email from that specific domain?
* Create a new inbound mail policy with a message filter that overrides Talos.
* Ask the user to add the sender to the email application&#8217;s allow list.
* Modify the firewall to allow emails from the domain.
* Add the domain into the allow list.
The allow list is a feature that allows Cisco ESA to accept messages from specific email addresses or domains, regardless of their sender-based reputation score or other reputation filters.

To allow inbound email from that specific domain, the administrator should add the domain into the allow list on Cisco ESA, which can be done from the web user interface by selecting Security Services > Safelist/Blocklist and clicking Add Entry.

The other options are not valid solutions to allow inbound email from that specific domain, because they do not affect the sender-based reputation score or the reputation filters on Cisco ESA.

NO.62 What is the order of virus scanning when multilayer antivirus scanning is configured?
* The default engine scans for viruses first and the McAfee engine scans for viruses second.
* The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.
* The McAfee engine scans for viruses first and the default engine scans for viruses second.
* The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.



Scanning Messages with Multiple Anti-Virus Scanning Engines

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

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

You cannot configure the order of virus scanning. When you enable multi-layer anti-virus scanning McAfee engine scans for viruses first, and the Sophos engine scans for viruses second. If the McAfe determines that a message is virus-free, the Sophos engine scans the message, adding a second laye protection. If the McAfee engine determines that a message contains a virus, the Cisco appliance skip 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

NO.63 When the Cisco ESA is configured to perform antivirus scanning, what is the default timeout value?
* 30 seconds
* 90 seconds
* 60 seconds
* 120 seconds
When Cisco ESA is configured to perform antivirus scanning, the default timeout value is 60 seconds, which means that Cisco ESA will wait for 60 seconds for the antivirus engine to scan a message before applying the configured action for unscannable messages, such as deliver, drop, or quarantine.

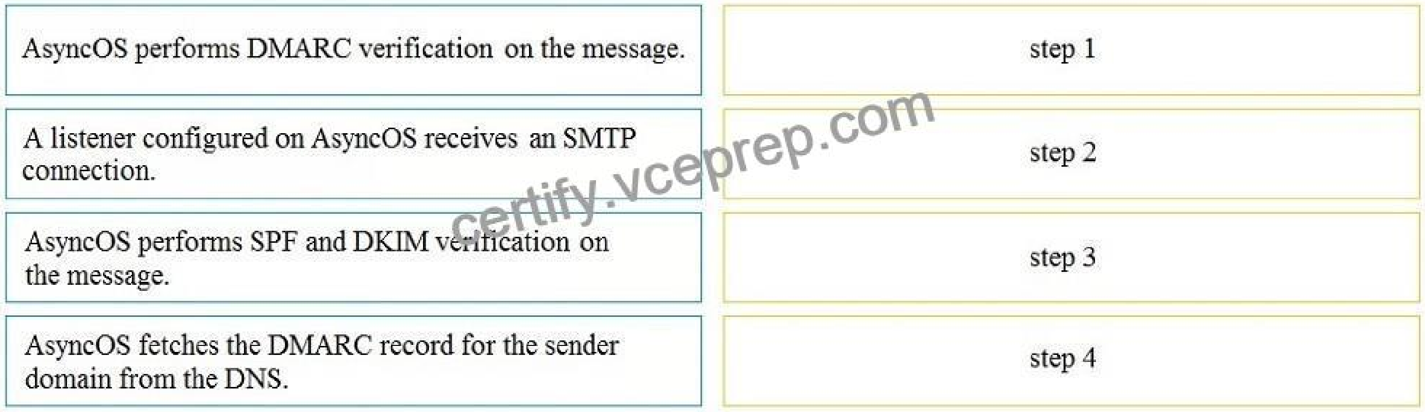
NO.64 Which components are required when encrypting SMTP with TLS on a Cisco Secure Email Gateway appliance when the sender requires TLS verification?
* DER certificate and matching public key from a CA
* self-signed certificate in PKCS#7 format
* X. 509 certificate and matching private key from a CA
* self-signed certificate in PKCS#12 format
To encrypt SMTP with TLS on a Cisco Secure Email Gateway appliance when the sender requires TLS verification, the components that are required are an X.509 certificate and matching private key from a CA. The certificate must be signed by a trusted CA and contain the domain name or IP address of the listener in the Subject or Subject Alternative Name fields. The private key must be unencrypted and match the certificate. Reference: [Cisco Secure Email Gateway Administrator Guide &#8211; Configuring TLS]

NO.65 Which two statements about configuring message filters within the Cisco ESA are true? (Choose two.)
* The filters command executed from the CLI is used to configure the message filters.
* Message filters configuration within the web user interface is located within Incoming Content Filters.
* The filterconfig command executed from the CLI is used to configure message filters.

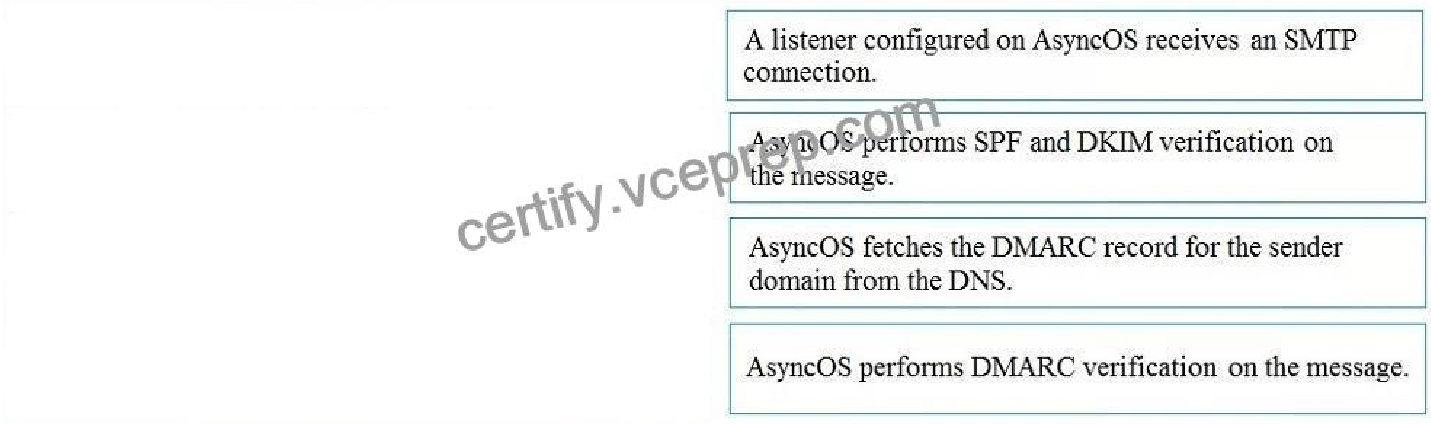
- Message filters can be configured only from the CLI.
- Message filters can be configured only from the web user interface.

NO.66 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



A listener configured on AsyncOS receives an SMTP connection.

AsyncOS performs SPF and DKIM verification on the message.

AsyncOS fetches the DMARC record for the sender domain from the DNS.

AsyncOS performs DMARC verification on the message.

NO.67 Which setting affects the aggressiveness of spam detection?

- protection level
- spam threshold
- spam timeout
- maximum depth of recursion scan

NO.68 Which two action types are performed by Cisco ESA message filters? (Choose two.)

- non-final actions
- filter actions
- discard actions
- final actions
- quarantine actions

Actual 300-720 Exam Recently Updated Questions with Free Demo: https://www.vceprep.com/300-720-latest-vce-prep.html]