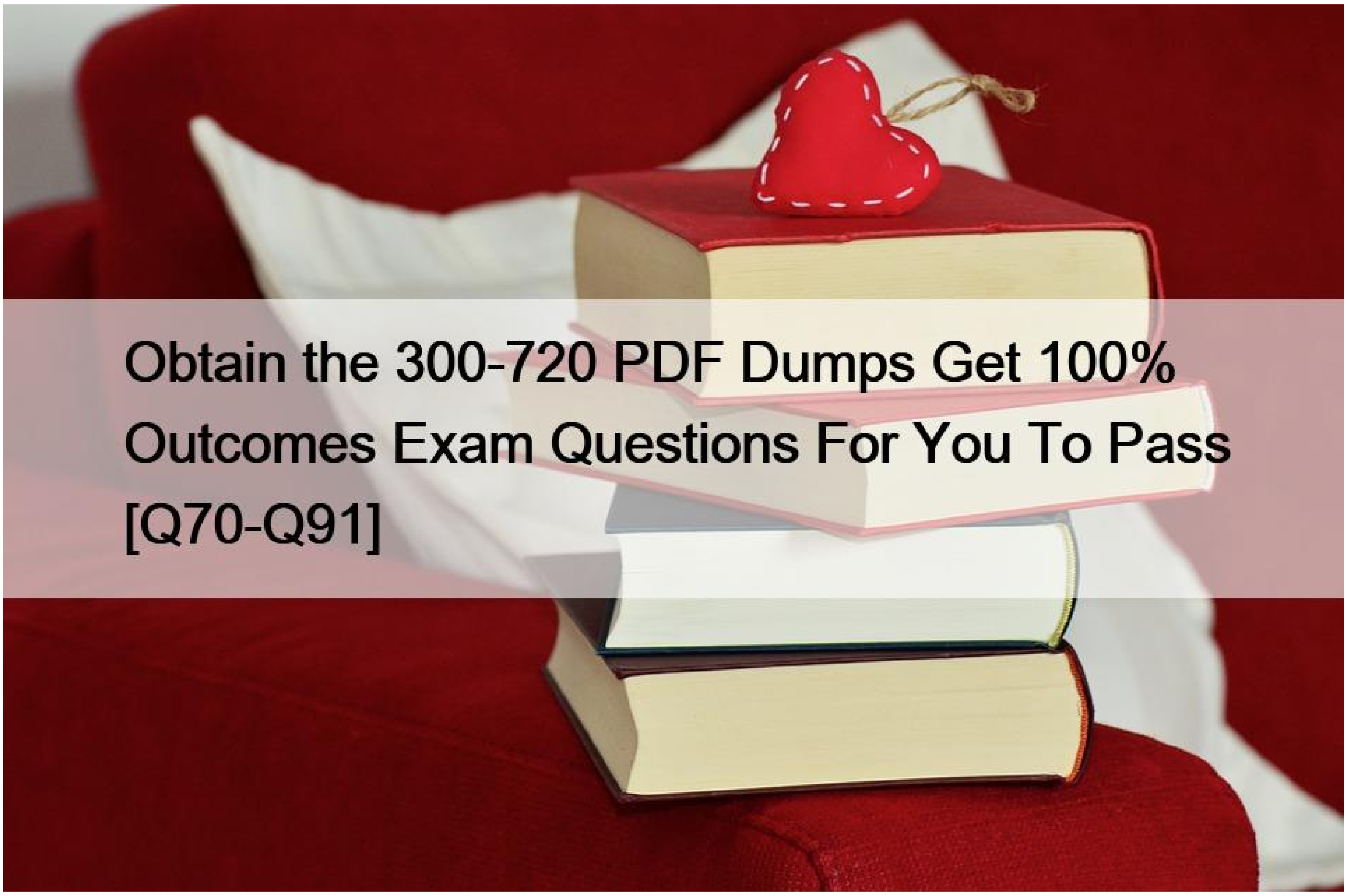
Obtain the 300-720 PDF Dumps Get 100% Outcomes Exam Questions For You To Pass [Q70-Q91



Obtain the 300-720 PDF Dumps Get 100% Outcomes Exam Questions For You To Pass
300-720 Exam Dumps Contains FREE Real Quesions from the Actual Exam

Cisco 300-720 certification is highly valued by employers, as it validates the candidate's expertise in securing email systems. Securing Email with Cisco Email Security Appliance certification demonstrates that the candidate has a deep understanding of email security appliances and can effectively implement and manage them in various network environments. Securing Email with Cisco Email Security Appliance certification also proves that the candidate is committed to continuous learning and professional development, as they have passed a rigorous exam that tests their abilities in a highly specialized area of expertise.

Cisco 300-720 certification exam consists of 60-70 questions that must be completed within 90 minutes. 300-720 exam covers a wide range of topics, including email security architecture, content security, message filters, and email authentication. Passing this certification exam requires a deep understanding of email security concepts and Cisco Email Security Appliance functionalities. Once you pass the exam, you will join the ranks of certified professionals who are recognized for their expertise in securing email with the Cisco Email Security Appliance.

Q70. When outbreak filters are configured, which two actions are used to protect users from outbreaks?

(Choose two.)
* redirect
* return
* drop
* delay
* abandon
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_01110.html

Q71. When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)
* redirect
* return
* drop
* delay
* abandon
The Outbreak Filters feature uses three tactics to protect your users from outbreaks:

Delay.

Redirect.

Modify.

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_01110.html

Q72. A network administrator enabled McAfee antivirus scanning on a Cisco Secure Email Gateway and configured the virus scanning action of &#8220;scan for viruses only&#8221; If the scanner finds a virus in an attachment for an incoming email, what action will be applied to this message?
* The email and attachment are forwarded to the network administrator.
* No repair is attempted, and the attachment is either dropped or delivered
* The attachment is dropped and replaced with a &#8220;Removed Attachment&#8221; file
* The system will attempt to repair the attachment
If the McAfee antivirus scanning is enabled on the Cisco Secure Email Gateway and the virus scanning action is set to &#8220;scan for viruses only&#8221;, then no repair is attempted, and the attachment is either dropped or delivered based on the antivirus policy settings. The administrator can choose to drop or deliver the infected attachment by selecting the appropriate action in the antivirus policy. Reference: [Cisco Secure Email Gateway Administrator Guide &#8211; Configuring McAfee Antivirus Scanning]

Q73. What is a benefit of implementing URL filtering on the Cisco ESA?
* removes threats from malicious URLs
* blacklists spam
* provides URL reputation protection
* enhances reputation against malicious URLs

Q74. What is the default HTTPS port when configuring spam quarantine on Cisco ESA?
* 83
* 82

* 443
* 80

Q75. 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

Q76. 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

Q77. An administrator needs to configure Cisco ESA to ensure that emails are sent and authorized by the owner of the domain. Which two steps must be performed to accomplish this task? (Choose two.)
* Generate keys.
* Create signing profile.
* Create Mx record.
* Enable SPF verification.
* Create DMARC profile.

Q78. An administrator is trying to enable centralized PVO but receives the error, &#8220;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.&#8221; 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.

Q79. An engineer is tasked with creating a content filter to catch attachments, including credit card numbers, and hold them for review until further action is taken. Which component on a Cisco Secure Email Gateway must be configured to meet this requirement?
* Spam Quarantine
* Policy Quarantine
* Outbreak Filter
* Content Filter

Content filter is a component on a Cisco Secure Email Gateway that must be configured to catch attachments, including credit card numbers, and hold them for review until further action is taken. Content filter allows you to define rules based on message content and apply actions such as quarantine, encrypt, or modify. Reference = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances &#8211; GD (General Deployment) &#8211; Content Filters [Cisco Secure Email Gateway] &#8211; Cisco]

Q80. Which two steps are needed to disable local spam quarantine before external quarantine is enabled? (Choose two.)

* Uncheck the Enable Spam Quarantine check box.
* Select Monitor and click Spam Quarantine.
* Check the External Safelist/Blocklist check box.
* Select External Spam Quarantine and click on Configure.
* Select Security Services and click Spam Quarantine.

To disable local spam quarantine before external quarantine is enabled on Cisco ESA, two steps are needed:

Select Security Services and click Spam Quarantine, which will open the Spam Quarantine settings page.

Uncheck the Enable Spam Quarantine check box, which will disable the local spam quarantine feature on Cisco ESA.

Q81. 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?

* Virus Infected Messages
* Unscannable Messages
* Encrypted Messages
* Positively Identified Messages

Q82. Which feature must be configured before an administrator can use the outbreak filter for nonviral threats?

* quarantine threat level
* antispam
* data loss prevention
* antivirus

The feature that must be configured before an administrator can use the outbreak filter for nonviral threats is antispam. The outbreak filter relies on the antispam engine to detect and block nonviral threats, such as phishing, malware, or spam campaigns. You need to enable antispam scanning and configure the antispam settings before you can use the outbreak filter.

Q83. Which SMTP extension does Cisco ESA support for email security?

* ETRN
* UTF8SMTP
* PIPELINING
* STARTTLS

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_011000.html

Q84. 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

End user safelist is a feature that allows end users to specify email addresses or domains that they want to receive messages from, regardless of the spam verdict or action assigned by Cisco ESA. Messages from senders on the end user safelist are delivered to the end user&#8217;s inbox without any spam filtering.

Q85. The company security policy requires that the finance department have an easy way to apply encryption to their outbound

messages that contain sensitive data Users must be able to flag the messages that require encryption versus a Cisco Secure Email Gateway appliance scanning all messages and automatically encrypting via detection Which action enables this capability?
* Create an encryption profile with [SECURE] in the Subject setting and enable encryption on the mail flow policy
* Create an outgoing content filter with no conditions and with the Encrypt and Deliver Now action configured with [SECURE] in the Subject setting
* Create an encryption profile and an outgoing content filter that includes [SECURE] within the Subject Header: Contains condition along with the Encrypt and Deliver Now action
* Create a DLP policy manager message action with encryption enabled and apply it to active DLP policies for outgoing mail.
According to the [Cisco Secure Email Encryption Service Add-In User Guide], you can create an encryption profile that defines the encryption settings and options for your encrypted messages[2, p. 11]. You can also create an outgoing content filter that applies the encryption profile to the messages that match certain conditions, such as having [SECURE] in the subject header[2, p. 12]. This way, you can allow users to flag the messages that require encryption by adding [SECURE] to the subject line.

The other options are not valid because:

A) Creating an encryption profile with [SECURE] in the Subject setting and enabling encryption on the mail flow policy will not work, as the Subject setting in the encryption profile is used to specify the subject line of the encrypted message envelope, not the original message[2, p. 11].

B) Creating an outgoing content filter with no conditions and with the Encrypt and Deliver Now action configured with [SECURE] in the Subject setting will not work, as this will encrypt all outgoing messages regardless of whether they have [SECURE] in the subject line or not[2, p. 12].

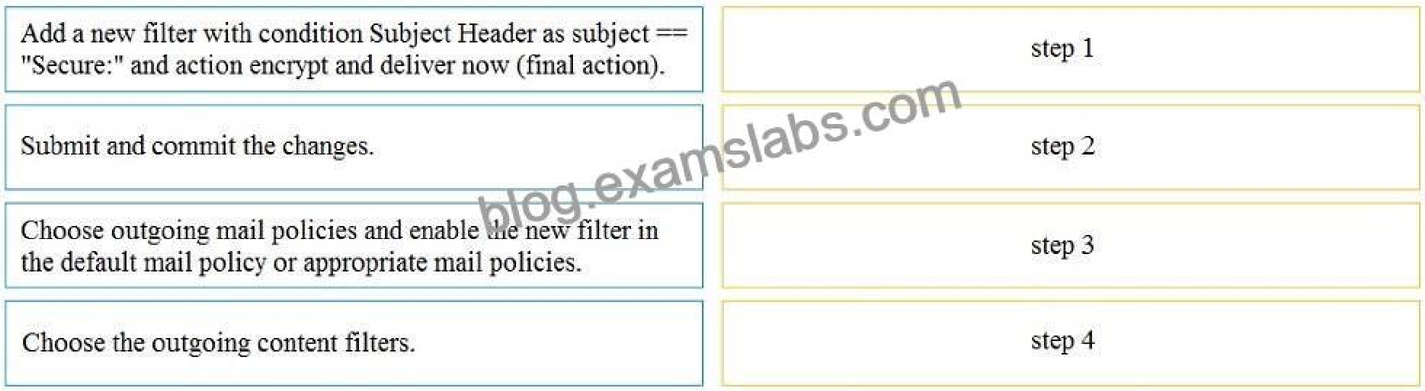
D) Creating a DLP policy manager message action with encryption enabled and applying it to active DLP policies for outgoing mail will not work, as this will encrypt messages based on DLP rules that detect sensitive data in the message content, not based on user flags in the subject line.

Q86. Users have been complaining of a higher volume of emails containing profanity. The network administrator will need to leverage dictionaries and create specific conditions to reduce the number of inappropriate emails.

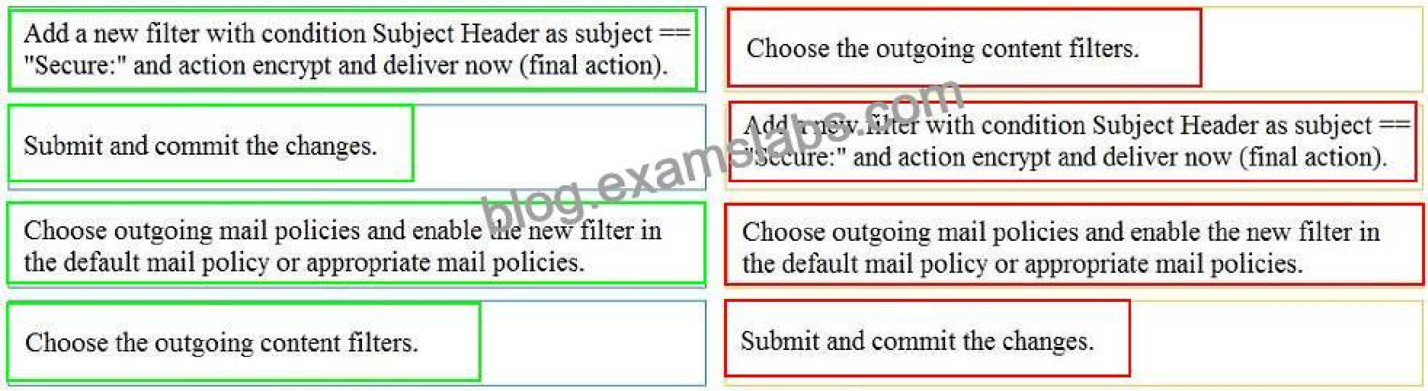
Which two filters should be configured to address this? (Choose two.)
* message
* spam
* VOF
* sender group
* content

Q87. 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 &#8220;Secure:&#8221; into the correct order on the right.



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



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

Reference:

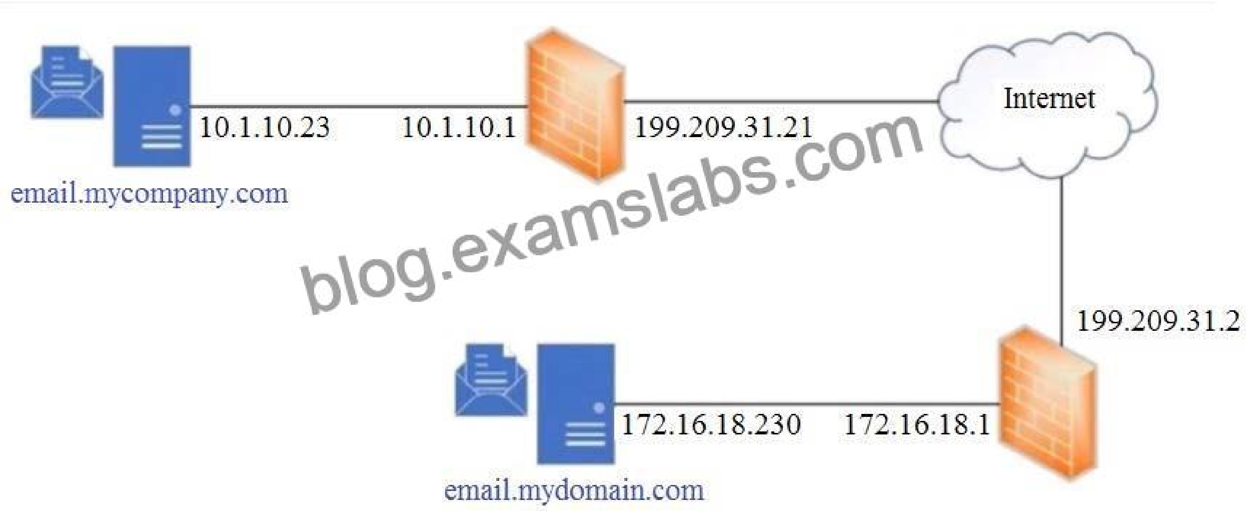
https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/td-p/2441383

Q88. Which two features are applied to either incoming or outgoing mail policies? (Choose two.)
* Indication of Compromise
* application filtering
* outbreak filters
* sender reputation filtering
* antivirus

Q89. When DKIM signing is configured, which DNS record must be updated to load the DKIM public signing key?
* AAAA record
* PTR record
* TXT record
* MX record

When DKIM (DomainKeys Identified Mail) signing is configured on Cisco ESA, the DNS record that must be updated to load the DKIM public signing key is the TXT record. The TXT record is used to store arbitrary text information in the DNS, such as the DKIM public key, which can be retrieved by the recipients to verify the DKIM signature in the message header.

Q90. Refer to the exhibit.



Which SPF record is valid for mycompany.com?
* v=spf1 a mx ip4:199.209.31.2 -all
* v=spf1 a mx ip4:10.1.10.23 -all
* v=spf1 a mx ip4:199.209.31.21 -all
* v=spf1 a mx ip4:172.16.18.230 -all

Q91. When a network engineer is troubleshooting a mail flow issue, they discover that some emails are rejected with an SMTP code of 451 and the error message &#8220;#4.7.1 Unable to perform DMARC verification&#8221;. In the DMARC verification profile on the Cisco Secure Email Gateway appliance, which action must be set for messages that result in temporary failure to prevent these emails from being rejected?
* Accept
* Ignore
* Quarantine
* No Action
Accept is the action that must be set for messages that result in temporary failure to prevent these emails from being rejected. Accept allows Cisco ESA to deliver the messages without applying any DMARC actions or modifications.

To configure the accept action for messages that result in temporary failure on Cisco ESA, the administrator can follow these steps:

Select Mail Policies > DMARC Verification Profile and click Edit Settings for the DMARC verification profile that applies to the messages.

Under DMARC Actions, select Accept from the drop-down menu for Messages That Result in Temporary Failure.

Click Submit.

The other options are not valid actions for messages that result in temporary failure to prevent these emails from being rejected, because they either apply DMARC actions or modifications or do nothing.

Use Real Cisco Achieve the 300-720 Dumps - 100% Exam Passing Guarantee:
https://www.examslabs.com/Cisco/CCNP-Security/best-300-720-exam-dumps.html]