

[February-2023Free 300-720 Dumps Offered by Braindump2go[Q46-Q76]

February/2023 Latest Braindump2go 300-720 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go 300-720 Real Exam Questions!
QUESTION 46Which two statements about configuring message filters within the Cisco ESA are true? (Choose two.)
A. The filters command executed from the CLI is used to configure the message filters.
B. Message filters configuration within the web user interface is located within Incoming Content Filters.
C. The filterconfig command executed from the CLI is used to configure message filters.
D. Message filters can be configured only from the CLI.
E. Message filters can be configured only from the web user interface.
Answer: AD
Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213940-esa-using-a-message-filter-to-take-act.html>

QUESTION 47What occurs when configuring separate incoming mail policies?
A. message splintering
B. message exceptions
C. message detachment
D. message aggregation
Answer: A
QUESTION 48Which default port is used by the Cisco ESA to quarantine the message on the Cisco Security Management Appliance?
A. port 25/TCP
B. port 110/TCP
C. port 443/TCP
D. port 6025/TCP
E. port 4766/UDP
Answer: D
QUESTION 49When configuring CRES, where do you enable read receipts?
A. In the encryption profile
B. In the content filter condition menu
C. In the content filter action menu
D. In the mail policy
Answer: A
QUESTION 50Which type of query must be configured when setting up the Spam Quarantine while merging notifications?
A. Spam Quarantine Alias Routing Query
B. Spam Quarantine Alias Consolidation Query
C. Spam Quarantine Alias Authentication Query
D. Spam Quarantine Alias Masquerading Query
Answer: B
QUESTION 51Which two factors must be considered when message filter processing is configured? (Choose two.)
A. message-filter order
B. lateral processing
C. structure of the combined packet
D. mail policies
E. MIME structure of the message
Answer: AE
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_chapter_01000.html

QUESTION 52How does the graymail safe unsubscribe feature function?
A. It strips the malicious content of the URI before unsubscribing.
B. It checks the URI reputation and category and allows the content filter to take an action on it.
C. It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.
D. It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.
Answer: D
Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200383-Graymail-Detection-and-Safe-Unsubscribing.html>

QUESTION 53Which 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 54An 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:



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

QUESTION 55Which feature must be configured before an administrator can use the outbreak filter for nonviral threats?
A. quarantine threat level
B. antispam
C. data loss prevention
D. antivirus
Answer: B
Explanation:By default, the Outbreak Filters feature scans your incoming and outgoing messages for possible viruses during an outbreak. You can enable scanning for non-viral threats in addition to virus outbreaks if you enable anti-spam scanning on the appliance.

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

QUESTION 56Which type of attack is prevented by configuring file reputation filtering and file analysis features?
A. denial of service
B. zero-day
C. backscatter
D. phishing
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_chapter_010000.html#con_1809885

QUESTION 57Which two service problems can the Cisco Email Security Appliance solve? (Choose two.)
A. DLP
B. IPSC
C. Antispam
D. URL filtering
Answer: AC
QUESTION 58Which of

the following types of DNS records deals with mail delivery for a specific domain?A. AB. TXTC. MXD. PTRAnswer: C
QUESTION 59When DKIM signing is configured, which DNS record must be updated to load the DKIM public signing key?A. AAAA recordB. PTR recordC. TXT recordD. MX recordAnswer: CExplanation:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa-configure-dkim-signing.html>QUESTION

60Which attack is mitigated by using Bounce Verification?A. spoofB. denial of serviceC. eavesdroppingD. smurfAnswer: B
Explanation:<https://www.networkworld.com/article/2305394/ironport-adds-bounce-back-verification-for-e-mail.html>QUESTION 61

When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)A. redirectB. returnC. dropD. delayE. abandonAnswer: ADEExplanation: The Outbreak Filters feature uses three tactics to protect your users from outbreaks:- Delay. Outbreak Filters quarantines messages that may be part of a virus outbreak or non-viral attack. While quarantined, the appliances receives updated outbreak information and rescans the message to confirm whether it's part of an attack.- Redirect. Outbreak Filters rewrites the URLs in non-viral attack messages to redirect the recipient through the Cisco web security proxy if they attempt to access any of the linked websites. The proxy displays a splash screen that warns the user that the website may contain malware, if the website is still operational, or displays an error message if the website has been taken offline. See Redirecting URLs for more information on redirecting URLs.- Modify. In addition to rewriting URLs in non-viral threat messages, Outbreak Filters can modify a message's subject and add a disclaimer above the message body to warn users about the message's content. See Modifying Messages for more information.QUESTION 62Which two features are applied to either incoming or outgoing mail policies? (Choose two.)A. Indication of CompromiseB. application filteringC. outbreak filtersD. sender reputation filteringE. antivirusAnswer: CEExplanation:

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_01001.htmlQUESTION 63What must be configured to allow the Cisco ESA to encrypt an email using the Cisco Registered

Envelope Service?A. provisioned email encryption profileB. message encryption from a content filter that select "Message Encryption" over TLS.C. message encryption from the mail flow policies with "CRES" selectedD. content filter to forward the email to the Cisco Registered Envelope serverAnswer: AExplanation:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-cres-encryption.pdf>QUESTION 64Which two configurations are used on multiple LDAP servers to connect with Cisco ESA? (Choose two.)A. load balancingB. SLA monitorC.

active-standbyD. failoverE. active-activeAnswer: ADQUESTION 65What is the default port to deliver emails from the Cisco

ESA to the Cisco SMA using the centralized Spam Quarantine?A. 8025B. 6443C. 6025D. 8443Answer: CQUESTION 66

Which two steps are needed to disable local spam quarantine before external quarantine is enabled? (Choose two.)A. Uncheck the Enable Spam Quarantine check box.B. Select Monitor and click Spam Quarantine.C. Check the External Safelist/Blocklist check box.D. Select External Spam Quarantine and click on Configure.E. Select Security Services and click Spam Quarantine.Answer: ABQUESTION 67Drag and Drop Question

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.	step 1
Configure a filter to take necessary action on SPF/SIDF verification results.	step 2
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	step 3
Test the results of message verification.	step 4
Configure a sendergroup to use the custom mail-flow policy.	step 5

Answer:

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.
Associate the filter with a nominated incoming mail policy.
Configure a sendergroup to use the custom mail-flow policy.
Test the results of message verification.

QUESTION 68 Drag and Drop Question 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.

Add a new filter with condition "Secure:" and action

Submit and commit the changes.

Choose outgoing mail policy and enable the default mail policy.

Choose the outgoing content filters.

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.

QUESTION 69 Drag and Drop Question Drag and drop the Cisco ESA reactions to a possible DLP from the left onto the correct action types on the right.

drop

encrypt messages

quarantine

deliver

send a copy to a policy quarantine

add a disclaimer

Primary Actions

Answer:

Primary Actions

deliver

drop

quarantine

send a copy to a policy quarantine

encrypt messages

add a disclaimer

QUESTION 70 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.

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.

step 1

step 2

step 3

step 4

Answer:

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.

QUESTION 71 A network administrator is modifying an outgoing mail policy to enable domain protection for the organization. A DNS entry is created that has the public key. Which two headers will be used as matching criteria in the outgoing mail policy? (Choose two.)
A. message-ID
B. sender
C. URL reputation
D. from
E. mail-from
Answer: BD
QUESTION 72 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?
A. Virus Infected Messages
B. Unscannable Messages
C. Encrypted Messages
D. Positively Identified Messages
Answer: C
QUESTION 73 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.
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_0100000.html#task_1749146

QUESTION 74 A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy. What is the reason of this?
A. The From* header is checked against all policies in a top-down fashion.
B. The message header with the highest priority is checked against each policy in a top-down fashion.
C. The To* header is checked against all policies in a top-down fashion.
D. The message header with the highest priority is checked against the Default policy in a top-down fashion.
Answer: D
QUESTION 75 An administrator identifies that, over the past week, the Cisco ESA is receiving many emails from certain senders and domains which are being consistently quarantined. The administrator wants to ensure that these senders and domain are unable to send anymore emails. Which feature on Cisco ESA should be used to achieve this?
A. incoming mail policies
B. safelist
C. blocklist
D. S/MIME Sending Profile
Answer: A
QUESTION 76 An engineer is testing mail flow on a new Cisco ESA and notices that messages for domain abc.com are stuck in the delivery queue. Upon further investigation, the engineer notices that the messages pending delivery are destined for 192.168.1.11, when they should instead be routed to 192.168.1.10. What configuration change needed to address this issue?
A. Add an address list for domain abc.com.
B. Modify Destination Controls entry for the domain abc.com.
C. Modify the SMTP route for the domain and change the IP address to 192.168.1.10.
D. Modify the Routing Tables and add a route for IP address to 192.168.1.10.
Answer: C
Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html>
Resources From: 1. 2023 Latest Braindump2go 300-720 Exam Dumps (PDF & VCE) Free Share: <https://www.braindump2go.com/300-720.html>
2. 2023 Latest Braindump2go 300-720 PDF and 300-720 VCE Dumps Free Share: https://drive.google.com/drive/folders/1CWQxEgDC6s96s0xdef_OXd8TQRMEIfP0?usp=sharing
Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!