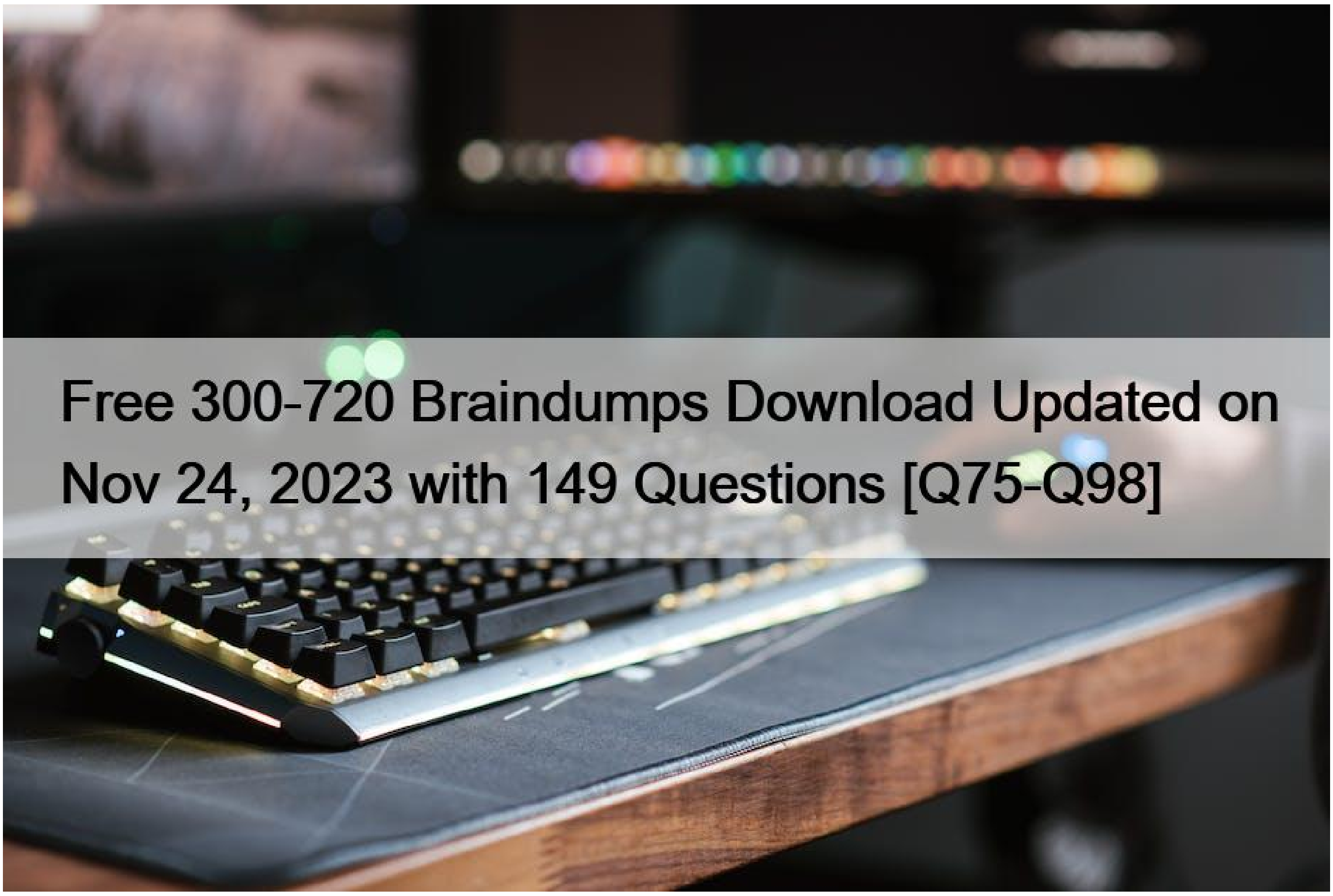
Free 300-720 Braindumps Download Updated on Nov 24, 2023 with 149 Questions [Q75-Q98



Free 300-720 Braindumps Download Updated on Nov 24, 2023 with 149 Questions
Cisco 300-720 Exam Practice Test Questions

Q75. Which Cisco ESA security service is configured only through an outgoing mail policy?
* antivirus
* DLP
* Outbreak Filters
* AMP

DLP (Data Loss Prevention) is a security service that is configured only through an outgoing mail policy on Cisco ESA. DLP allows Cisco ESA to scan outgoing messages for sensitive or confidential data, such as credit card numbers, social security numbers, health records, etc., and apply appropriate actions, such as encrypt, quarantine, notify, etc., to prevent data leakage or loss.

Reference:

Reference https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_01001.html

Q76. 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.

Message filters can only be applied to the ESA via command line. So, you will need command line access to the ESA.

Log into the ESA via command line.

Run the following highlighted commands to apply the message filter to the ESA:

```
ironport.example.com> filters

Choose the operation you want to perform:

&#8211; NEW &#8211; Create a new filter.

&#8211; IMPORT &#8211; Import a filter script from a file.

[]> NEW

Enter filter script. Enter &#8216;.&#8217; on its own line to end.

large_spam_no_attachment:

if ((body-size > 2097152) AND NOT (attachment-size > 0)) {

quarantine(&#8220;large_spam&#8221;);

log-entry(&#8220;*****This is a large message with no attachments*****&#8221;);

}

.

1 filters added.
```

Q77. 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

Q78. An organization wants to designate help desk personnel to assist with tickets that request the release of messages from the spam quarantine because company policy does not permit direct end-user access to the quarantine. Which two roles must be used to allow help desk personnel to release messages while restricting their access to make configuration changes in the Cisco Secure

Email Gateway? (Choose two.)
* Administrator
* Help Desk User
* Read-Only Operator
* Technician
* Quarantine Administrator

All users with administrator privileges can change spam quarantine settings and view and manage messages in the spam quarantine. You do not need to configure spam quarantine access for administrator users.

If you configure access to the spam quarantine for users with the following roles, they can view, release, and delete messages in the spam quarantine:

-Operator

-Read-only operator

-Help desk user

-Guest

-Custom user roles that have spam quarantine privileges

These users cannot access spam quarantine settings.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_0100000.html?bookSearch=true#con_1624156

Q79. 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.

Q80. A security administrator deployed a Cisco Secure Email Gateway appliance with a mail policy configured to store suspected spam for review. The appliance is the DMZ and only the standard HTTP/HTTPS ports are allowed by the firewall. An administrator wants to ensure that users can view any suspected spam that was blocked. Which action must be taken to meet this requirement?
* Enable the external Spam Quarantine and enter the IP address and port for the Secure Email and Web Manager
* Enable the Spam Quarantine and leave the default settings unchanged.
* Enable End-User Quarantine Access and point to an LDAP server for authentication.
* Enable the Spam Quarantine and specify port 80 for HTTP and port 443 for HTTPS

Enabling End-User Quarantine Access and pointing to an LDAP server for authentication is the action that must be taken to meet this requirement. End-User Quarantine Access is a feature that allows users to access their personal quarantine on Cisco ESA using their email address and password, without requiring an administrator account or access to Secure Email and Web Manager.

To enable End-User Quarantine Access on Cisco ESA, the administrator can follow these steps:

Select Security Services > IronPort Anti-Spam > End User Safelist/Blocklist Settings and click Edit Settings.

Under End User Quarantine Access, select Enable End User Quarantine Access.

Under Authentication Server, select LDAP Server from the drop-down menu and choose an LDAP server profile from the drop-down menu.

Click Submit.

Q81. 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?
* Add an address list for domain abc.com.
* Modify Destination Controls entry for the domain abc.com.
* Modify the SMTP route for the domain and change the IP address to 192.168.1.10.
* Modify the Routing Tables and add a route for IP address to 192.168.1.10.

Q82. The CEO added a sender to a safelist but does not receive an important message expected from the trusted sender. An engineer evaluates message tracking on the Cisco Secure Email Gateway appliance and determines that the message was dropped by the antivirus engine. What is the reason for this behavior?
* The sender is included in an ISP blocklist
* Administrative access is required to create a safelist.
* The sender didn&#8217;t mark the message as urgent
* End-user safelists apply to antispam engines only.
The reason why the CEO did not receive an important message expected from a trusted sender after adding them to a safelist is because end-user safelists apply to antispam engines only. End-user safelists are lists of sender addresses or domains that end users can create and manage through their quarantine accounts or email clients. End-user safelists allow end users to accept or exempt messages from certain senders or domains from being identified as spam by the antispam engines. However, end-user safelists do not affect other filtering engines such as antivirus, outbreak filters, or content filters. Reference = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances &#8211; GD (General Deployment) &#8211; Safelists and Blocklists [Cisco Secure Email Gateway] &#8211; Cisco

Q83. 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

Q84. 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.
Explanation/Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa-

00.html (configuration summary)

Q85. Which process is skipped when an email is received from safedomain.com, which is on the safelist?
* message filter
* antivirus scanning
* outbreak filter
* antispam scanning
The safelist is a list of email addresses or domains that are considered legitimate and trustworthy by Cisco ESA. When an email is received from a sender on the safelist, Cisco ESA skips antispam scanning for that message and delivers it to the recipient without any spam filtering.

Q86. Which type of DNS record would contain the following line, which references the DKIM public key per RFC 6376?

v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A2362BECE40658267045694328 3BE
* CNAME
* AAAA
* TXT
* PTR
A TXT record is a type of DNS record that contains arbitrary text data that can be used for various purposes such as verification, configuration, or authentication. A TXT record can contain the DKIM public key per RFC 6376, which is used to verify the digital signature of an email message generated by the DKIM private key of the sender domain.

The other options are not valid because:

A) A CNAME record is a type of DNS record that maps an alias name to a canonical name or another alias name. It does not contain any DKIM public key information.

B) An AAAA record is a type of DNS record that maps a hostname to an IPv6 address. It does not contain any DKIM public key information.

D) A PTR record is a type of DNS record that maps an IP address to a hostname, which is the reverse of an A or AAAA record. It does not contain any DKIM public key information.

Q87. An organization has multiple Cisco Secure Email Gateway appliances deployed, resulting in several spam quarantines to manage. To manage the quarantined messages, the administrator enabled the centralized spam quarantine on the Cisco Secure Email and Web Manager appliance and configured the external spam quarantine on the Cisco Secure Email Gateway appliances. However, messages are still being directed to the local quarantine on the Cisco Secure Email Gateway appliances What change is necessary to complete the configuration?
* Modify the incoming mail policies on the Cisco Secure Email Gateway appliances to redirect to the external quarantine
* Disable the external spam quarantine on the Cisco Secure Email Gateway appliances
* Disable the local spam quarantine on the Cisco Secure Email Gateway appliances.
* Modify the external spam quarantine settings on the Cisco Secure Email Gateway appliances and change the port to 25
To use the centralized spam quarantine on the Cisco Secure Email and Web Manager appliance, the administrator must disable the local spam quarantine on the Cisco Secure Email Gateway appliances. This will prevent messages from being stored in both quarantines and avoid confusion for end users and administrators. Reference: [Cisco Secure Email and Web Manager User Guide &#8211; Configuring Centralized Spam Quarantine]

Q88. 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.
Explanation/Reference:

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

Q89. Which benefit does enabling external spam quarantine on Cisco SMA provide?
* ability to back up spam quarantine from multiple Cisco ESAs to one central console
* access to the spam quarantine interface on which a user can release, duplicate, or delete
* ability to scan messages by using two engines to increase a catch rate
* ability to consolidate spam quarantine data from multiple Cisco ESA to one central console
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-0/user_guide/b_SMA_Admin_Guide/b_SMA_Admin_Guide_chapter_010101.html

Q90. A Cisco Secure Email Gateway administrator is creating a Mail Flow Policy to receive outbound email from Microsoft Exchange. Which Connection Behavior must be selected to properly process the messages?
* Accept
* Delay
* Relay
* Reject
Relay is the connection behavior that must be selected to properly process the messages. Relay allows Cisco ESA to accept messages from the specified source and deliver them to the intended destination, without applying any content or reputation filters.

To configure a mail flow policy with relay connection behavior on Cisco ESA, the administrator can follow these steps:

Select Mail Policies > Mail Flow Policies and click Add Policy.

Enter a name and description for the mail flow policy, such as Exchange Outbound.

Under Connection Behavior, select Relay.

Click Submit.

The other options are not valid connection behaviors to properly process the messages, because they either reject, delay, or accept the messages with content or reputation filters applied.

Q91. Which benefit does enabling external spam quarantine on Cisco SMA provide?
* ability to back up spam quarantine from multiple Cisco ESAs to one central console
* access to the spam quarantine interface on which a user can release, duplicate, or delete
* ability to scan messages by using two engines to increase a catch rate
* ability to consolidate spam quarantine data from multiple Cisco ESA to one central console

Q92. Which functionality is impacted if the assigned certificate under one of the IP interfaces is modified?
* traffic between the Cisco Secure Email Gateway and the LDAP server

* emails being delivered from the Cisco Secure Email Gateway
* HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway
* emails being received by the Cisco Secure Email Gateway
If the assigned certificate under one of the IP interfaces is modified, then the HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway will be impacted. The administrator must ensure that the certificate is valid and trusted by the browser or client that is used to access the web user interface. Otherwise, the connection may fail or generate a warning message. Reference: [Cisco Secure Email Gateway Administrator Guide &#8211; Configuring Certificates]

Q93. 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?
* incoming mail policies
* safelist
* blocklist
* S/MIME Sending Profile

Q94. 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.
Reference:

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

Q95. Which Cisco Secure Email Threat Defense visibility and remediation mode is only available when using Cisco Secure Email Gateway as the message source?
* Basic Authentication
* No Authentication
* Microsoft 365 Authentication
* Cisco Security Cloud Sign On
According to the Cisco Secure Email Threat Defense User Guide, the No Authentication option is only available if you are using a Cisco Secure Email Gateway (SEG) as your message source. This option allows visibility only, no remediation1.

The other options are not valid because:

A) Basic Authentication is not a visibility and remediation mode for Cisco Secure Email Threat Defense. It is a method of authenticating users with a username and password2.

C) Microsoft 365 Authentication is a visibility and remediation mode that allows you to use Microsoft 365 credentials to access Cisco Secure Email Threat Defense. It has two sub-options: Read/Write and Read. This mode is available for both Microsoft 365 and Gateway message sources1.

D) Cisco Security Cloud Sign On is not a visibility and remediation mode for Cisco Secure Email Threat Defense. It is a service that manages user authentication for Cisco security products, including Cisco Secure Email Threat Defense3.

Q96. What is the default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine?
* 8025
* 6443
* 6025
* 8443

Q97. Spreadsheets containing credit card numbers are being allowed to bypass the Cisco ESA.

Which outgoing mail policy feature should be configured to catch this content before it leaves the network?
* file reputation filtering
* outbreak filtering
* data loss prevention
* file analysis

Q98. 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&#8217; 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
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_010001.html#task_140

94

Updated Verified 300-720 dumps Q&As - Pass Guarantee or Full Refund:
https://www.test4engine.com/300-720_exam-latest-braindumps.html]