DUMPSHQ

Free Questions for 300-720 by dumpshq

Shared by Day on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is a category for classifying graymail?

Options:

A- Malicious

B- Marketing

C- Spam

D- Priority

Answer:

B

Explanation:

According to the [Cisco Secure Email User Guide], graymail is a category of email messages that are not spam but may be unwanted by some recipients, such as newsletters, promotions, or social media updates[5, p. 25]. Marketing is one of the subcategories of graymail that includes messages that advertise products or services[5, p. 26].

The other options are not valid because:

A) Malicious is not a category for classifying graymail. It is a category for classifying email messages that contain malicious content such as malware, phishing, or fraud[5, p. 25].

C) Spam is not a category for classifying graymail. It is a category for classifying email messages that are unsolicited, unwanted, or harmful[5, p. 25].

D) Priority is not a category for classifying graymail. It is a category for classifying email messages that are important, urgent, or relevant[5, p. 25].

Question 2

Question Type: MultipleChoice

An engineer wants to utilize a digital signature in outgoing emails to validate to others that the email they are receiving was indeed sent and authorized by the owner of that domain Which two components should be configured on the Cisco Secure Email Gateway appliance to achieve this? (Choose two.)

Options:

A- DMARC verification profile

B- SPF record

C- Public/Private keypair

D- Domain signing profile

E- PKI certificate

Answer:

C, D

Explanation:

Public/Private keypair. A public/private keypair is a pair of cryptographic keys that are used to generate and verify digital signatures. The private key is used to sign the email message, while the public key is used to verify the signature. The public key is published in a DNS record, while the private key is stored on the Cisco Secure Email Gateway appliance[1, p. 2].

Domain signing profile. A domain signing profile is a configuration that specifies the domain and selector to use for signing outgoing messages, as well as the signing algorithm, canonicalization method, and header fields to include in the signature. You can create multiple domain signing profiles for different domains or subdomains[1, p. 3].

The other options are not valid because:

A) DMARC verification profile is not a component for utilizing a digital signature in outgoing emails. It is a component for verifying the authenticity of incoming emails based on SPF and DKIM results[2, p. 1].

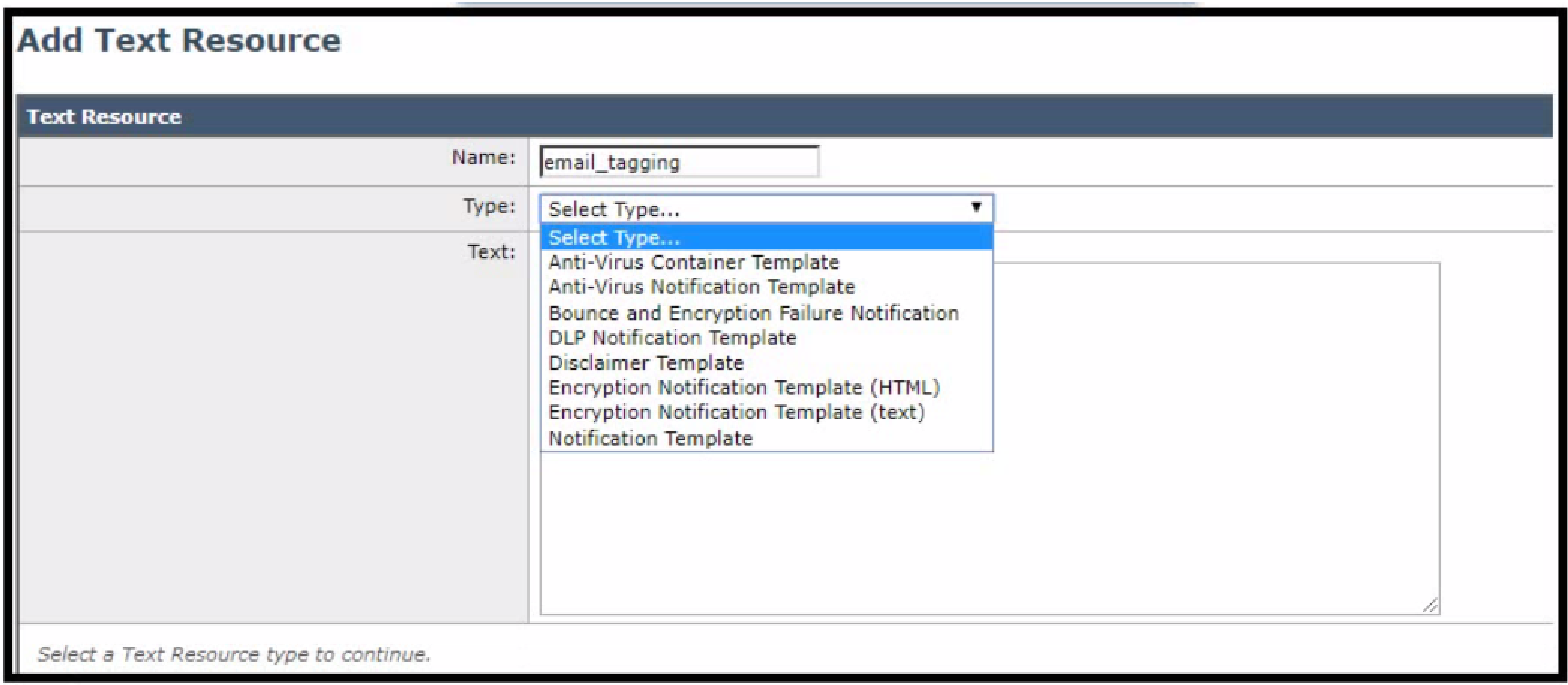
B) SPF record is not a component for utilizing a digital signature in outgoing emails. It is a component for validating the sender IP address of incoming emails based on a list of authorized IP addresses published in a DNS record[3, p. 1].

E) PKI certificate is not a component for utilizing a digital signature in outgoing emails. It is a component for encrypting and decrypting email messages based on a certificate authority that issues and validates certificates[4, p. 1].

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



Add Text Resource

Text Resource

Name: email_tagging

Type: Select Type...

Text:

Select Type...
Anti-Virus Container Template
Anti-Virus Notification Template
Bounce and Encryption Failure Notification
DLP Notification Template
Disclaimer Template
Encryption Notification Template (HTML)
Encryption Notification Template (text)
Notification Template

Select a Text Resource type to continue.

For improved security, an administrator wants to warn users about opening any links or attachments within an email How must the administrator configure an HTML-coded message at the top of an email body to create this warning?

Options:

A- Create a text resource type of Disclaimer Template paste the HTML code into the text box. then use this text resource inside a content filter

B- Create a text resource type of Disclaimer Template change to code view to paste the HTML code into the text box, then use this text resource inside a content filter

C- Create a text resource type of Notification Template, paste the HTML code into the text box, then use this text resource inside a content filter.

D- Create a text resource type of Notification Template, change to code view to paste the HTML code into the text box. then use this text resource inside a content filter.

Answer:

B

Explanation:

According to the [Cisco Secure Email User Guide], you can create a text resource of type Disclaimer Template and use the code view option to insert HTML code into the text box. Then, you can use this text resource in a content filter to prepend or append the HTML message to the email body[1, p. 15-16].

The other options are not valid because:

A) Creating a text resource type of Disclaimer Template and pasting the HTML code into the text box without changing to code view will not work, as the HTML code will be treated as plain text and not rendered properly[1, p. 15].

C) Creating a text resource type of Notification Template and pasting the HTML code into the text box will not work, as Notification Templates are used for sending notifications to senders or recipients, not for modifying the email body[1, p. 17].

D) Creating a text resource type of Notification Template and changing to code view to paste the HTML code into the text box will not work, as Notification Templates are used for sending notifications to senders or recipients, not for modifying the email body[1, p. 17].

Question 4

Question Type: MultipleChoice

An engineer tries to implement phishing simul-ations to test end users, but they are being blocked by the Cisco Secure Email Gateway appliance. Which two components, when added to the allow list, allow these simul-ations to bypass antispam scanning? (Choose two.)

Options:

A- domains

B- senders

C- reputation score

D- receivers

E- spf check

Answer:

A, B

Explanation:

To allow phishing simul-ations to bypass antispam scanning, the administrator must add two components to the allow list: domains and senders. Domains are the email domains that are used in the phishing simulations, such as example.com or test.com. Senders are the email addresses that are used to send the phishing simulations, such as phish@example.com or test@test.com. By adding these components to the allow list, the administrator can prevent them from being blocked by antispam scanning and allow them to reach the end users for testing purposes.Reference: [Cisco Secure Email Gateway Administrator Guide - Creating Allow Lists]

Question 5

Question Type: MultipleChoice

Which Cisco Secure Email Threat Defense visibility and remediation mode is only available when using Cisco Secure Email Gateway as the message source?

Options:

A- Basic Authentication

B- No Authentication

C- Microsoft 365 Authentication

D- Cisco Security Cloud Sign On

Answer:

B

Explanation:

According to theCisco 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.

Question 6

Question Type: **MultipleChoice**

Which feature must be activated on a Cisco Secure Email Gateway to combat backscatter?

Options:

A- Graymail Detection

B- Bounce Verification

C- Forged Email Detection

D- Bounce Profile

Answer:

B

Explanation:

To combat backscatter, which is a type of spam that consists of bounce messages sent to forged sender addresses, the administrator must enable the Bounce Verification feature under Security Settings. This feature allows the appliance to verify whether a bounce message is legitimate or not by checking if the original message was sent from the appliance. If not, the bounce message is considered as backscatter and can be dropped or quarantined.Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Bounce Verification]

Question 7

Question Type: **MultipleChoice**

An engineer wants to ensure that emails received by company users that contain URLs do not make them susceptible to data loss from accessing malicious or undesired external content sources Which two features must be configured on Cisco Secure Email Gateway to meet this requirement1? (Choose two.)

Options:

A- antispam scanning

B- data loss prevention

C- graymail detection

D- URL filtering

E- antivirus scanning

Answer:

A, D

Explanation:

To meet the requirement of ensuring that emails received by company users that contain URLs do not make them susceptible to data loss from accessing malicious or undesired external content sources, the administrator must configure two features on Cisco Secure Email Gateway: antispam scanning and URL filtering. Antispam scanning can block or quarantine messages that are identified as spam based on various criteria, such as sender reputation, message content, and message headers. URL filtering can rewrite or defang URLs in messages that are associated with malicious or undesirable websites, such as phishing, malware, adult, or gambling sites.Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Antispam Scanning] and [Cisco Secure Email Gateway Administrator Guide - Configuring URL Filtering]

Question 8

Question Type: MultipleChoice

An administrator notices that the Cisco Secure Email Gateway delivery queue on an appliance is consistently full. After further investigation, it is determined that the IP addresses currently in use by appliance are being rate-limited by some destinations. The administrator creates a new interface with an additional IP address using virtual gateway technology, but the issue is not solved Which configuration change resolves the issue?

Options:

A- Use the CLI command altsrchost to set the new interface as the source IP address for all mail.

B- Use the CLI command loadbalance auto to enable mail delivery over all interfaces.

C- Use the CLI command alt-src-host to set the new interface as a possible delivery candidate.

D- Use the CLI command deliveryconfig to set the new interface as the primary interface for mail delivery

Answer:

D

Explanation:

Determining Which Interface is Used for Mail Delivery Unless you specify the output interface via the deliveryconfig</code> command or via a message filter (alt-src-host), or through the use of a virtual gateway, the output interface is selected by the AsyncOS routing table. 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_011001.html?bookSearch=true

Question 9

Question Type: **MultipleChoice**

What is the default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHCP server is not available?

Options:

A- Manual configuration of an IP address is required through the serial port before remote access

B- DHCP is required for the initial IP address assignment

C- Use the IP address of 192.168 42 42 via the Management port

D- Manual configuration of an IP address is required through the hypervisor console before remote access

Answer:

C

Explanation:

The default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHCP server is not available is to use the IP address of 192.168.42.42 via the Management port. This IP address is assigned by default to the Management port of the virtual gateway and can be used to access the web user interface or the command-line interface of the appliance.Reference: [Cisco Secure Email Gateway Installation and Upgrade Guide - Configuring Network Settings]

Question 10

Question Type: **MultipleChoice**

Which action do Outbreak Filters take to stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites?

Options:

A- Rewrite URLs to redirect traffic to potentially harmful websites through a web security proxy

B- Block all emails from email domains associated with potentially harmful websites.

C- Strip all attachments from email domains associated with potentially harmful websites.

D- Quarantine messages that contain links to potentially harmful websites until the site is taken offline

Answer:

A

Explanation:

Outbreak Filters can take the action of rewriting URLs to redirect traffic to potentially harmful websites through a web security proxy. This allows the Cisco Secure Email Gateway to scan the content of the websites and block or warn the user if they are malicious or undesirable. This action can stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites, that may not be detected by other filters.Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring Outbreak Filters]

20%
DISCOUNT