Cisco.300-720.v2026-07-08.q95

Exam Code:	300-720
Exam Name:	Securing Email with Cisco Email Security Appliance
Certification Provider:	Cisco
Free Question Number:	95
Version:	v2026-07-08
# of views:	105
# of Questions views:	1024
https://www.freecram.net/torrent/Cisco.300-720.v2026-07-08.q95.html	

NEW QUESTION: 1
Which action must be taken before a custom quarantine that is being used can be deleted?
A. Delete the quarantine that is assigned to a filter.
B. Delete the quarantine that is not assigned to a filter.
C. Delete only the unused quarantine.
D. Remove the quarantine from the message action of a filter.
Answer: (SHOW ANSWER)
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.: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-5.
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_011111.html

NEW QUESTION: 2
What is the purpose of Cisco Email Encryption on Cisco ESA?
A. to ensure anonymity between a recipient and MTA
B. to ensure integrity between a sender and MTA
C. to aut henticate direct communication between a sender and Cisco ESA
D. to ensure privacy between Cisco ESA and MTA
Answer: (SHOW ANSWER)
Overview of Encrypting Communication with Other MTAs:
AsyncOS supports the STARTTLS extension to SMTP (Secure SMTP over TLS).
The TLS implementation in AsyncOS provides privacy through encryption.
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_011001.html?bookSearch=true

NEW QUESTION: 3

A network engineer is reviewing the record presented.

```
Name: big-email._domainkey.mywebsite.com
Data: v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBA0508877311VT
```

Which type of DNS record would contain the record as per the DKIM public key RFC 6376?

A. PTR

B. MX

C. SRV

D. TXT

Answer: (SHOW ANSWER)

NEW QUESTION: 4

What is a benefit of graymail services?

A. provides the option to unsubscribe from unwanted marketing emails

B. removes spam based on the sender email address

C. offers cloud and on-site unsubscription service

D. provides a safe method to subscribe to social network emails

Answer: (SHOW ANSWER)

NEW QUESTION: 5

Which Cisco ESA security service is configured only through an outgoing mail policy?

A. antivirus

B. DLP

C. Outbreak Filters

D. AMP

Answer: (SHOW ANSWER)

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.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 9-2.

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

NEW QUESTION: 6

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

A. No Authentication

B. Basic Authentication

C. Cisco Security Cloud Sign On

D. Microsoft 365 Authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 7

An administrator manipulated the subnet mask but was still unable to access the user interface. How must the administrator access the Cisco Secure Email Gateway appliance to perform the initial configuration?

A. Use the serial or console port

B. Use the management port

C. Use the data 2 port

D. Use the data 1 port

Answer: (SHOW ANSWER)

If you are unable to access the user interface of the Cisco Secure Email Gateway appliance after manipulating the subnet mask, you can use the serial or console port to perform the initial configuration. The serial or console port provides a command-line interface that allows you to configure basic network settings such as IP address, subnet mask, gateway, and hostname 3 . References = User Guide for AsyncOS 12.0 for Cisco Email Security Appli ances - GD (General Deployment) - Configuring Network Settings [Cisco Secure Email Gateway] - Cisco

NEW QUESTION: 8

When email authentication is configured on Cisco ESA, which two key types should be selected on the signing profile? (Choose two.)

A. DKIM

B. Public Keys

C. Domain Keys

D. Symmetric Keys

E. Private Keys

Answer: (SHOW ANSWER)

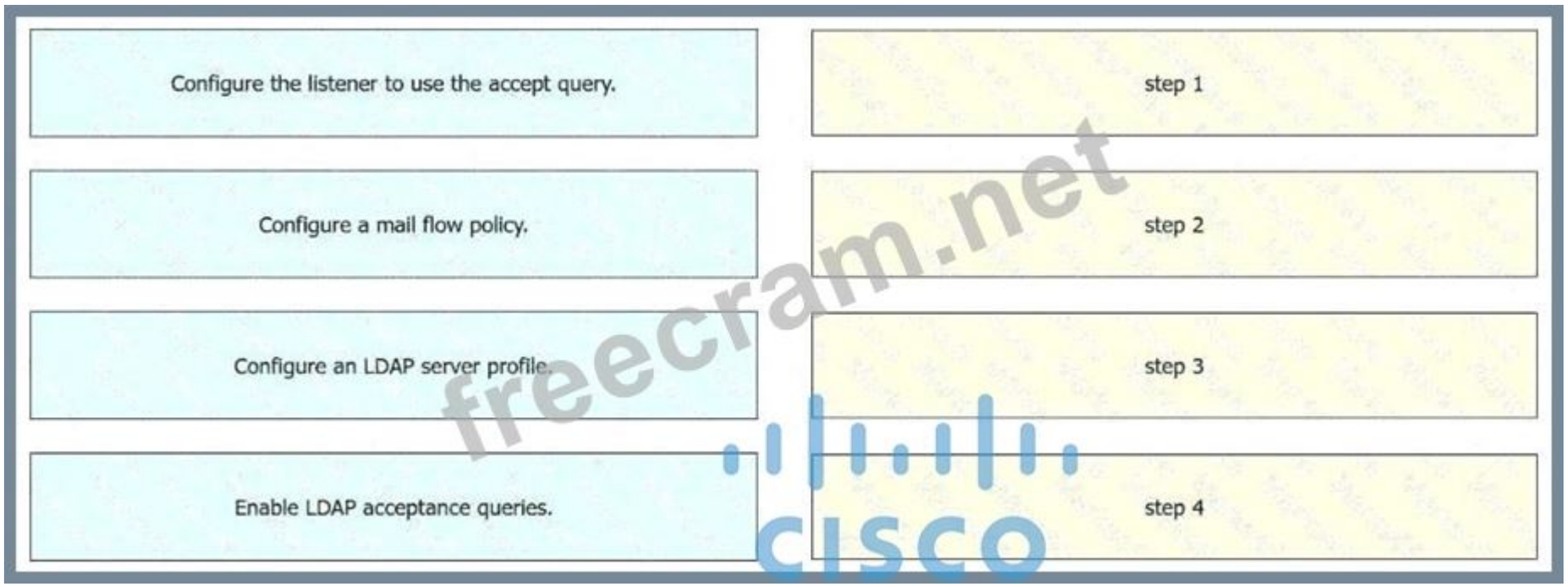
With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography.

Configuring DomainKeys and DKIM Signing A signing key is the private key stored on the appliance.

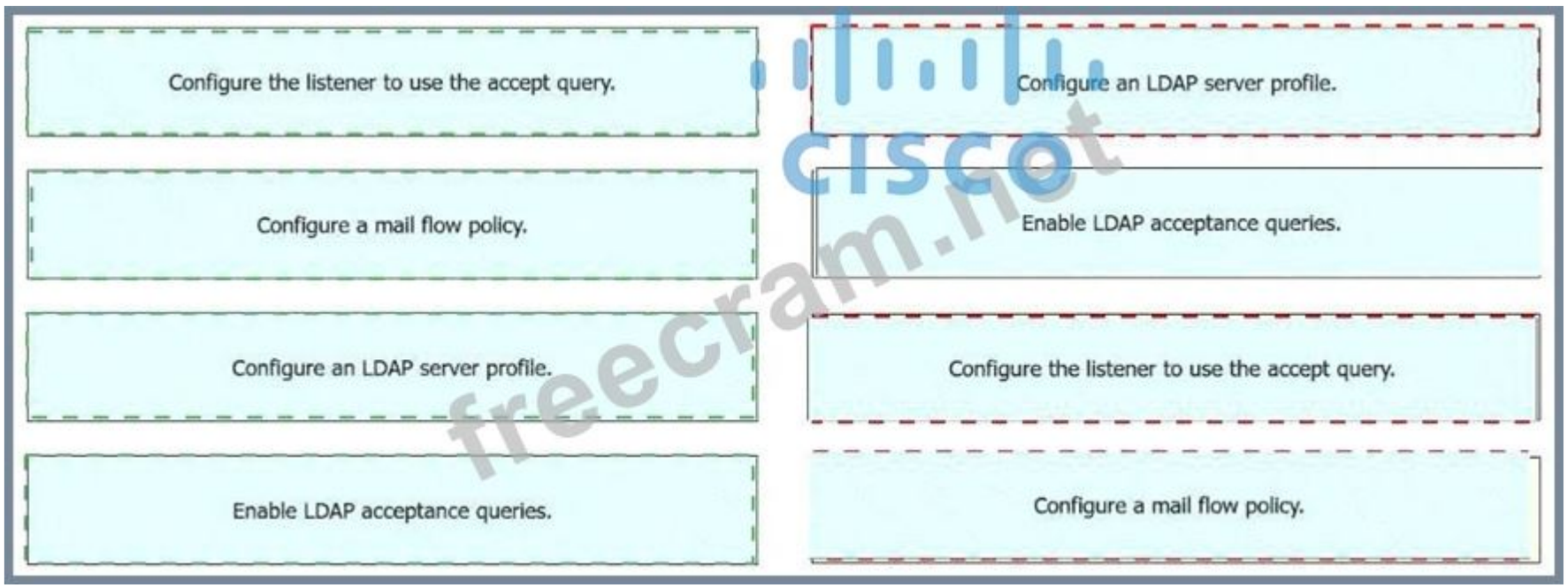
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_010101.html?bookSearch=true

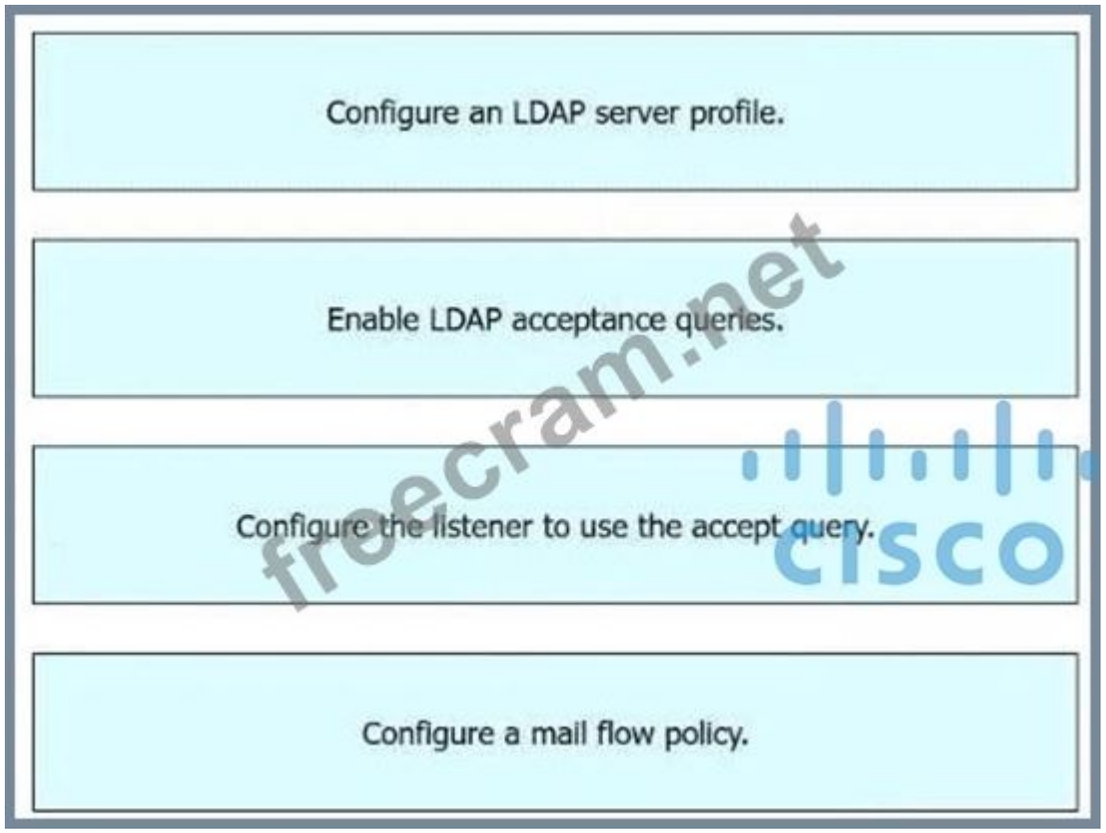
NEW QUESTION: 9

Drag and drop the actions from the left into the sequence on the right to configure directory harvest prevention in Cisco Secure Email Gateway.


Configure the listener to use the accept query.
Configure a mail flow policy.
Configure an LDAP server profile.
Enable LDAP acceptance queries.
step 1
step 2
step 3
step 4

Answer:


Configure the listener to use the accept query.
Configure a mail flow policy.
Configure an LDAP server profile.
Enable LDAP acceptance queries.
Configure an LDAP server profile.
Enable LDAP acceptance queries.
Configure the listener to use the accept query.
Configure a mail flow policy.



NEW QUESTION: 10

An engineer must configure a mail policy for all incoming email that contains a Microsoft Excel attachment.
All such email must be quarantined without any exception. After the incoming mail policy is created, which action must be taken next to meet the requirement?

A. Configure the Outgoing Content Filters settings.
B. Set the quarantine threat level threshold to 5.
C. Set the quarantine threat level threshold to 1.
D. Create an incoming content filter to match required attachments.
Answer: (SHOW ANSWER)

NEW QUESTION: 11

A recent engine update was pulled down for graymail and has caused the service to start crashing. It is critical to fix this as quickly as possible.
What must be done to address this issue?

A. Roll back to a previous version of the engine from the Services Overview page.
B. Roll back to a previous version of the engine from the System Health page.
C. Download another update from the IMS and Graymail page.
D. Download another update from the Service Updat es page.
Answer: (SHOW ANSWER)

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_11_1_chapter_0100010.html#task_9F07A032042F48C6AEDB69D325CD3C5F

To address this issue, the administrator should roll back to a previous version of the engine from the Services Overview page on Cisco ESA. This will restore the functionality of graymail service and prevent it from crashing.
The Services Overview page allows the administrator to view and manage various services on Cisco ESA, such as antivirus, outbreak filters, graymail, etc., and perform actions such as enable/disable, update, or roll back.
The other options are not valid solutions to address this issue, because they do not allow the administrator to roll back to a previous version of the engine for graymail service.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-18 and page 6-19.

NEW QUESTION: 12
An engineer must configure a virtual gateway on a Cisco Secure Email Gateway to send email for a group named GroupInt. GroupInt is part of these domains:
*domain 1 -lab
*domain2.lab
Drag and drop the code snippets from the right onto the boxes to configure the virtual gateway. Not all options are used.

```
example.lab> interfaceconfig
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> [          ]
Choose the operation you want to perform:
- NEW - Create a new group.
[]> NEW
Enter the name for this group.
[]> GroupInt
Enter the name or number of the interfaces to be included in this group.
Separate your choices with commas or specify a range with a dash.
1. data1 (10.66.71.12/24: c150b.lab)
2. Domain1 (192.168.1.1/24 on Data 1: domain1.lab)
3. Domain2 (192.168.2.1/24, 2001:db8::/32 on Data 1: domain2.lab)
[1]> [          ]
Group GroupInt created.
Currently configured IP groups:
1. GroupInt (Domain1, Domain2)
example.lab> altsrchost
Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
[]> [          ]
Which interface do you want to send messages for @test.com from?
1. data1 (10.66.71.12/24: c150b.lab)
2. Domain1 (192.168.1.1/24 on Data 1: domain1.lab)
3. Domain2 (192.168.2.1/24, 2001:db8::/32 on Data 1: domain2.lab)
IP Groups:
4. GroupInt (Domain1, Domain2)
[1]> [          ]
```

Data	import	edit	2,3
new	GROUPS	4	

Answer:

```
example.lab> interfaceconfig
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> GROUPS
Choose the operation you want to perform:
- NEW - Create a new group.
[]> NEW
Enter the name for this group.
[]> GroupInt
Enter the name or number of the interfaces to be included in this group.
Separate your choices with commas or specify a range with a dash.
1. data1 (10.66.71.12/24: c150b.lab)
2. Domain1 (192.168.1.1/24 on Data 1: domain1.lab)
3. Domain2 (192.168.2.1/24, 2001:db8::/32 on Data 1: domain2.lab)
[1]> 2,3
Group GroupInt created.
Currently configured IP groups:
1. GroupInt (Domain1, Domain2)
example.lab> altsrchost
Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
[]> new
Which interface do you want to send messages for @test.com from?
1. data1 (10.66.71.12/24: c150b.lab)
2. Domain1 (192.168.1.1/24 on Data 1: domain1.lab)
3. Domain2 (192.168.2.1/24, 2001:db8::/32 on Data 1: domain2.lab)
IP Groups:
4. GroupInt (Domain1, Domain2)
[1]> 4
```

Data | import | edit | 2,3

new | GROUPS | 4

```
example.lab> interfaceconfig
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> GROUPS
Choose the operation you want to perform:
- NEW - Create a new group.
[]> NEW
Enter the name for this group.
[]> GroupInt
Enter the name or number of the interfaces to be included in this group.
Separate your choices with commas or specify a range with a dash.
1. data1 (10.66.71.12/24: c150b.lab)
2. Domain1 (192.168.1.1/24 on Data 1: domain1.lab)
3. Domain2 (192.168.2.1/24, 2001:db8::/32 on Data 1: domain2.lab)
[1]> 2,3
Group GroupInt created.
Currently configured IP groups:
1. GroupInt (Domain1, Domain2)
example.lab> altsrchost
Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
[]> new
Which interface do you want to send messages for @test.com from?
1. data1 (10.66.71.12/24: c150b.lab)
2. Domain1 (192.168.1.1/24 on Data 1: domain1.lab)
3. Domain2 (192.168.2.1/24, 2001:db8::/32 on Data 1: domain2.lab)
IP Groups:
4. GroupInt (Domain1, Domain2)
[1]> 4
```


NEW QUESTION: 13

```
TEST: if (forged-email-detection ("support", 60)) { fed("from", ""); }
```

Refer to the exhibit. An engineer needs to change the existing Forged Email Detection message filter so that it references a newly created dictionary named 'Executives'.

What should be done to accomplish this task?

A. Change " from " to " Executives " .

B. Change " TESF to " Executives " .

C. Change fed ' to " Executives " .

D. Change " support " to " Executives " .

Answer: (SHOW ANSWER)

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKSEC-2240.pdf

NEW QUESTION: 14

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?

A. Modify the incoming mail policies on the Cisco Secure Email Gateway appliances to redirect to the external quarantine

B. Disable the external spam quarantine on the Cisco Secure Email Gateway appliances

C. Disable the local spam quarantine on the Cisco Secure Email Gateway appliances.

D. Modify the external spam quarantine settings on the Cisco Secure Email Gateway appliances and change the port to 25

Answer: C (LEAVE A REPLY)

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 w ill prevent messages from being stored in both quarantines and avoid confusion for end users and administrators. References : [Cisco Secure Email and Web Manager User Guide - Configuring Centralized Spam Quarantine]

NEW QUESTION: 15

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 " #4.7.1 Unable to perform DMARC verification " . 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?

A. Accept

B. Ignore

C. Quarantine

D. No Action

Answer: (SHOW ANSWER)

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.

References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 11-4 and page 11-5.

NEW QUESTION: 16

An 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: (SHOW ANSWER)

The PVO cannot be enabled and shows this type of error message.

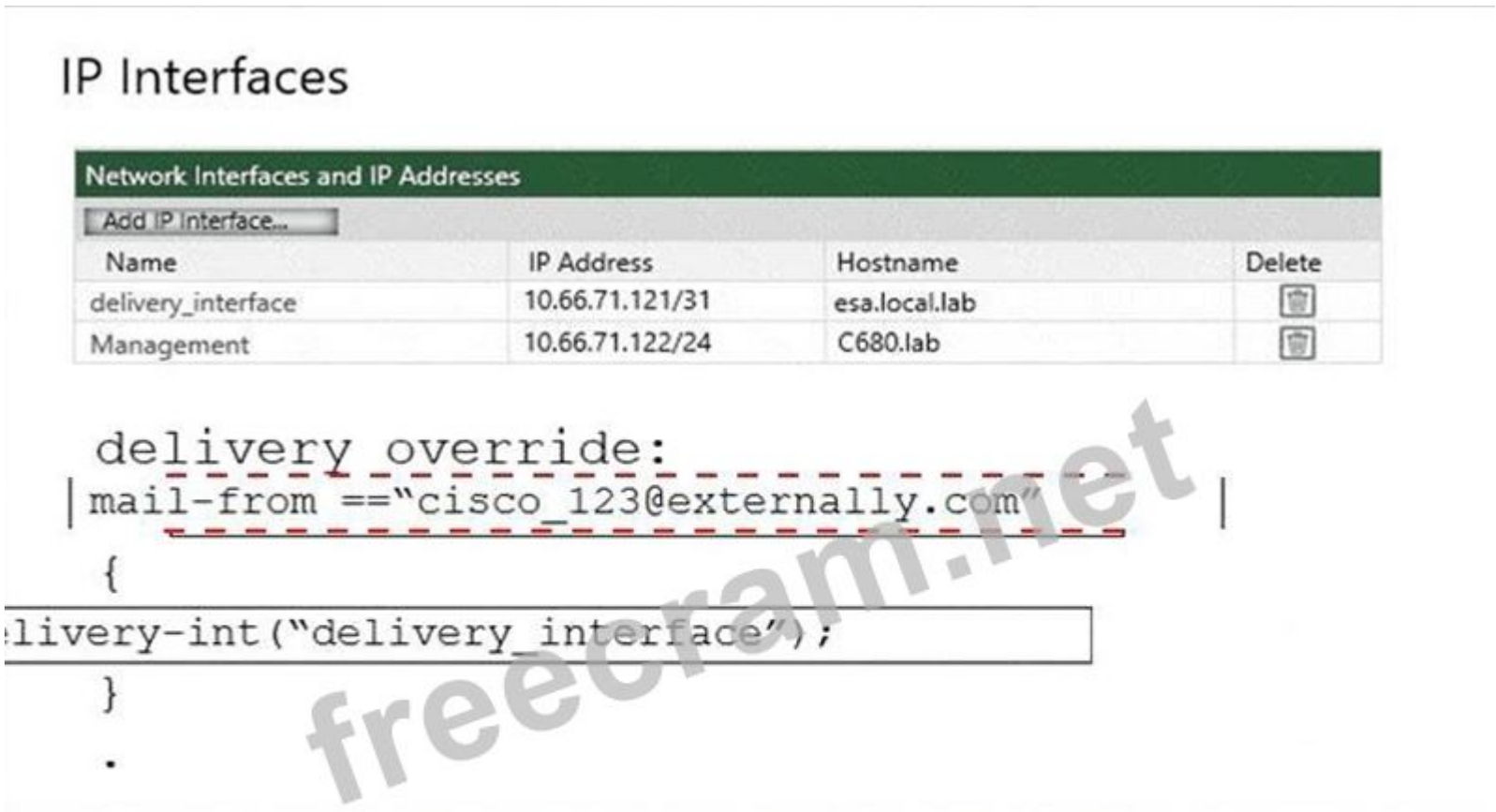
Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines configuration as host1 and host2 in Cluster have content filters / DLP actions available at a level different from the cluster Level.

The error message can indicate that one of the hosts does not have a DLP feature key applied and DLP is disabled. The solution is to add the missing feature key and apply DLP settings identical as on the host that has the feature key applied. This feature key inconsistency might have the same effect with Outbreak Filters, Sophos Antivirus, and other feature keys.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote- esa-00.html

NEW QUESTION: 17
A Cisco ESA administrator was notified that a user wa s 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?
A. Create a new inbound mail polic y with a message filter that overrides Talos.
B. Ask the user to add the sender to the email application ' s allow list.
C. Modify the firewall to allow emails from the domain.
D. Add the domain into the allow list.
Answer: (SHOW ANSWER)
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.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-13 and page 6-14.

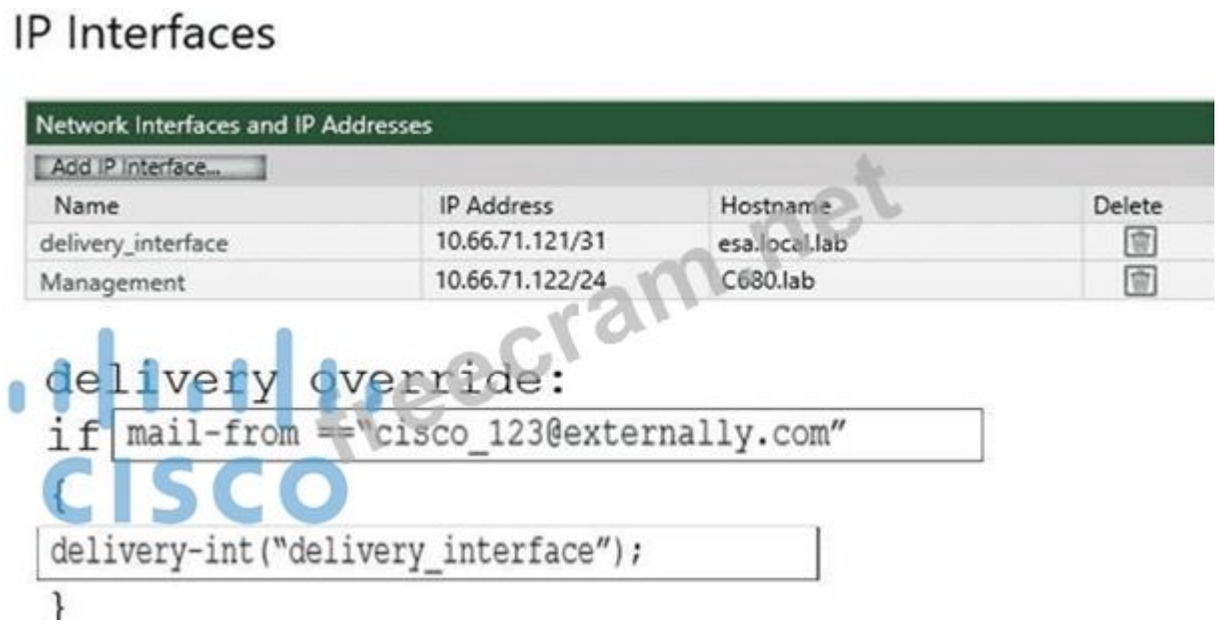
NEW QUESTION: 18
An administrator must ensure that emails sent from cisco_123@externally.com are routed through an alternate virtual gateway. Drag and drop the snippet from the bottom onto the blank in the graphic to finish the message filter syntax. Not all snippets are used.

Answer:



Explanation:

Table Description automatically generated



NEW QUESTION: 19
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?
A. The retention period was changed to one hour.
B. The threshold settings were set to override the clock se ttings.
C. The retention period was set to default.
D. The threshold settings were set to default.
Answer: (SHOW ANSWER)
You can configure Policy, Virus, and Outbreak Quarantines in any one of the following ways:
Choose Quarantine > Other Quarantine > View > +.
Choose Monitor > Policy, Virus, and Outbreak Quarantines and do one of the following.
Click Add Policy Quarantine.
Keep the following in mind, changing the retention time of the File Analysis quarantine from the default of one hour is not recommended.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guid e_14-0
/b_ESA_Admin_Guide_12_1_chapter_011111.html?bookSearch=true

NEW QUESTION: 20
Which functionality is impacted if the assigned certificate under one of the IP interfaces is modified?
A. traffic between the Cisco Secure Email Gateway and the LDAP server
B. emails being delivered from the Cisco Secure Email Gateway
C. HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway
D. emails being received by the Cisco Secure Email Gateway
Answer: (SHOW ANSWER)
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. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Certificates]

NEW QUESTION: 21
Which two steps configure Forged Email Detection? (Choose two.)
A. Configure a content dictionary with executive email addresses.
B. Configure a filter to use the Forged Email Detection rule and dictionary.
C. Configure a filter to check the Header From value against the Forged Email Detection dictionary.
D. Enable Forged Email Detection on the Security Services page.
E. Configure a content dictionary with friendly names.
Answer: B,E (LEAVE A REPLY)
Forged Email Detection is a feature that allows Cisco ESA to detect and block messages that spoof the display names of internal senders in the From header, such as executives or managers, to trick recipients into opening malicious or fraudulent emails. To configure this feature, two steps are required:
* Configure a content dictionary with friendly names of internal senders that should not appear in the From header of external messages, such as Alpha Beta or John Smith.
* Configure a filter to use the Forged Email Detection rule and dictionary, which will compare the display name in the From header of incoming messages with the entries in the content dictionary, and apply the configured action if a match is found.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 9-8.

NEW QUESTION: 22
Refer to the exhibit.

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	SPF-QUARANTINE-FAIL	SPF-QUARANTINE-FAIL: if (spf-status != "fail") { log-entry("*** SPF FAILED QUARANTINE ***"); quarantine("Policy"); skip-filters(); }		

A network engineer must set up a content filter to find any messages that failed SPF and send them into quarantine The content filter has been set up and enabled, but all messages except those that have failed SPF are being sent into quarantine. Which section of the filter must be modified to correct this behavior?
A. skip-filters
B. log-entry
C. spf-status
D. quarantine
Answer: (SHOW ANSWER)
spf-status is the section of the filter that must be modified to correct this behavior. spf-status is a condition that determines whether a message matches the content filter rule based on the result of SPF verification, such as pass, fail, neutral, etc.
The content filter in the exhibit has a spf-status condition set to "Pass", which means that it will match messages that passed SPF verification and apply the action of "Quarantine". This is the opposite of what the network engineer intended to do.
To correct this behavior, the network engineer can modify the spf-status condition to "Fail", which means that it will match messages that failed SPF verification and apply the action of "Quarantine".
The other options are not valid sections of the filter that must be modified to correct this behavior, because they do not affect the spf-status condition.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 8-3 and page 8-4.

NEW QUESTION: 23

An engineer must provide differentiated email filtering to executives within the organization Which two actions must be taken to accomplish this task? (Choose two)

A. Define an LDAP group query to specify users to whom the mail policy rules apply.

B. Create content filters for actions to take on messages that contain specific data

C. Upload a csv file containing the email addresses for the users for whom you want to create mail policies.

D. Enable the content-scanning features you want to use with mail policies

E. Define the default mail policies for incoming or outgoing messages

Answer: (SHOW ANSWER)

* Define an LDAP group query to specify users to whom the mail policy rules apply. This way, you can create a custom group of executive users and apply different mail policie s to them based on their LDAP attributes[4 , p. 2].

* Create content filters for actions to take on messages that contain specific data. Content filters allow you to scan the message body and attachments for keywords, phrases, or patterns that match your crit eria and perform actions such as quarantine, encrypt, or drop the message[4 , p. 7].

The other options are not valid because:

* C. Uploa ding a csv file containing the email addresses for the users for whom you want to create mail policies is not a supported feature of Cisco Secure Email 1 .

* D. Enabling the content-scanning features you want to use with mail policies is not necessary, as content scanning is enabled by default for all incoming and outgoing messages[4 , p. 6].

* E. Defining the default mail policies for incomin g or outgoing messages is not sufficient, as default mail policies apply to all users and do not allow for differentiation based on user groups[4 , p. 2].

NEW QUESTION: 24

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 a ddress to 192.168.1.10.

D. Modify the Routing Tables and add a route for IP address to 192.168.1.10.

Answer: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html

You can use the SMTP route feature on Cisco ESA to specify how messages for a specific domain are routed to their destination. You can modify the SMTP route for the domain abc.com and change the IP address to

192.168.1.10 to ensure that messages a re delivered correctly 3 . References = Securing Email with Cisco Email Security Appliance (SESA) v3.1

NEW QUESTION: 25

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.)

A. DMARC verification profile

B. SPF record

C. Public/Private keypair

D. Domain signing profile
E. PKI certificate
Answer: (SHOW ANSWER)
* 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 ke y 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 mes sages, 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 digi tal 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 signatu re 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].

NEW QUESTION: 26
When an email is sent with bounce verification enabled, which address is rewritten by the Cisco Secure Email Gateway in the message?
A. sender
B. envelope recipient
C. envelope sender
D. recipient
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which 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: (SHOW ANSWER)
The type of attack that is prevented by configuring file reputation filtering and file analysis features is zero- day. Zero-day attacks are those that exploit unknown vulnerabilities in software or systems before they are patched or fixed. File reputation filtering and file analysis features help to protect against zero-day attacks by checking the reputation of files attached to email messages and sending them to a cloud-based service for dynamic analysis.
References: Securing Email with Cisco Email Security Appliance (SESA) v3.1 , Module 9: Using Advanced Malware Protection, Lesson 1: Configuring File Reputation Filtering and File Analysis 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_010000.html#con_1809885

NEW QUESTION: 28

Which action is a valid fallback when a client certificate is unavailable during SMTP authentication on Cisco ESA?

A. LDAP Query

B. SMTP AUTH

C. SMTP TLS

D. LDAP BIND

Answer: (SHOW ANSWER)

SMTP AUTH is a valid fallback action when a client certificate is unavailable during SMTP authentication on Cisco ESA. SMTP AUTH is a method of authenticating SMTP clients using username and password credentials, which can be verified by an LDAP server or a local database on Cisco ESA.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 5-10.

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_011011.html

NEW QUESTION: 29

What occurs when configuring separate incoming mail policies?

A. message splintering

B. message exceptions

C. message detachment

D. message aggregation

Answer: (SHOW ANSWER)

Message splintering is a process that occurs when configuring separate incoming mail policies on Cisco ESA.

Message splintering means that Cisco ESA will split a single incoming message into multiple copies, each with a different recipient and policy, and apply different security services and actions to each copy.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , pag e 4-2.

NEW QUESTION: 30

An engineer must configure an incoming antispam mail policy in Cisco Secure Email Gateway for IT users.

The solution must meet these requirements: *The policy must be editable only by administrators.

*The policy must be activated for all incoming emails that are destined for admin@cisco.com .

These configurations have been performed already:

*Create an incoming mail policy.

*Set the name and the role to admin.

*Activate the antispam security service.

Which two additional actions must be taken to complete the configuration? (Choose two.)

A. Set Following Recipients to admin@.cisco com.

B. Configure the senders for the policy to any Sender.

C. Enable Following Senders to admm@cisco.com.

D. Configure the recipients for the policy to any Recipient.

E. Set Following Recipients to admin@cisco.com.

Answer: (SHOW ANSWER)

NEW QUESTION: 31

What is the default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine?

A. 8025

B. 6443

C. 6025

D. 8443

Answer: (SHOW ANSWER)

The default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine is 6025. This is the default value for the Port setting in the External Spam Quarantine configuration on Cisco ESA. This port must be open on both Cisco ESA and Cisco SMA for the communication to work.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-4.

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure- esa-00.html

NEW QUESTION: 32

An organization has a strict policy on URLs embedded in emails. The policy allows visibility into what the URL is but does not allow the user to click it. Which action must be taken to meet the requirements of the security policy?

A. Enable the URL quarantine policy

B. Defang the URL.

C. Replace the URL with text

D. Redirect the URL to the Cisco security proxy

Answer: (SHOW ANSWER)

To meet the security policy of allowing visibility into what the URL is but not allowing the user to click it, the administrator must defang the URL. This means that the URL will be modified in a way that it is still readable by humans but not clickable by browsers. For example, http://example.com could be defanged as hxxp://example[.]com.

References : [Cisco Secure Email Gateway Administrator Guide - Defanging URL s in Messages]

NEW QUESTION: 33

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

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: (SHOW ANSWER)

The default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHC P 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. References : [Cisco Secure Email Gateway Installation and Upgrade Guide - Configuring Network Settings]

NEW QUESTION: 34
A Cisco Secure Email Gateway administrator recently enabled the Outbreak Filters Global Service Setting to detect Viral as well as Non-Viral threat detection, with no detection of Non-viral threats after 24 hours of monitoring Outbreak Filters What is the reason that Non-Viral threat detection is not detecting any positive verdicts?
A. Non-Viral threat detection requires Antivirus or AMP enablement to properly function
B. The Outbreak Filters option Graymail Header must be enabled
C. Non-Viral threat detection requires AntiSpam or Intelligent Multi-Scan enablement to properly function.
D. The Outbreak Filters option URL Rewriting must be enabled.
Answer: (SHOW ANSWER)
According to the [Cisco Secure Email User Guide], Non-Viral threat detection is a feature of Outbreak Filters that detects a nd blocks email messages that contain non-viral threats such as phishing, fraud, or social engineering[1 , p. 25]. To use this feature, you need to enable either AntiSpam or Intelligent Multi-Scan on your Cisco Secure Email Gateway, as these features provid e the necessary scanning and filtering capabilities for Non-Viral threat detection[1 , p. 26].
The other options are not valid because:
* A. Non-Viral threat detection does not require Antivirus or AMP enablement to properly function.
Antivirus and AMP are features that detect and block email messages that contain viral threats such as malware or ransomware[1 , p. 27-28].
* B. The Outbreak Filters option Graymail Header does not affect Non-Viral threat detection. Graymail Header is an option that allows you to add a header to email messages that are classified as graymail, which are messages that are not spam but may be unwanted by some recipients, such as newsletters or promotions[1 , p. 25].
* D. The Outbreak Filters option URL Rewriting does not affect Non-Viral threat detection. URL Rewriting is an option that allows you to rewrite the URLs in email messages to point to a Cisco proxy server, which can scan the URLs for malicious content and redirect the users to a warning page if needed[1 , p. 25].

NEW QUESTION: 35
What is needed to sign outbound emails using Domain Keys Identified Mail after a signing profile is created in the Cisco Secure Email Gateway?
A. Configure in destination controls.
B. Enable DKIM in the mail flow policy.
C. Enable DKIM in an outbound content filter.
D. A signing profile referencing the sender domain is sufficient.
Answer: (SHOW ANSWER)

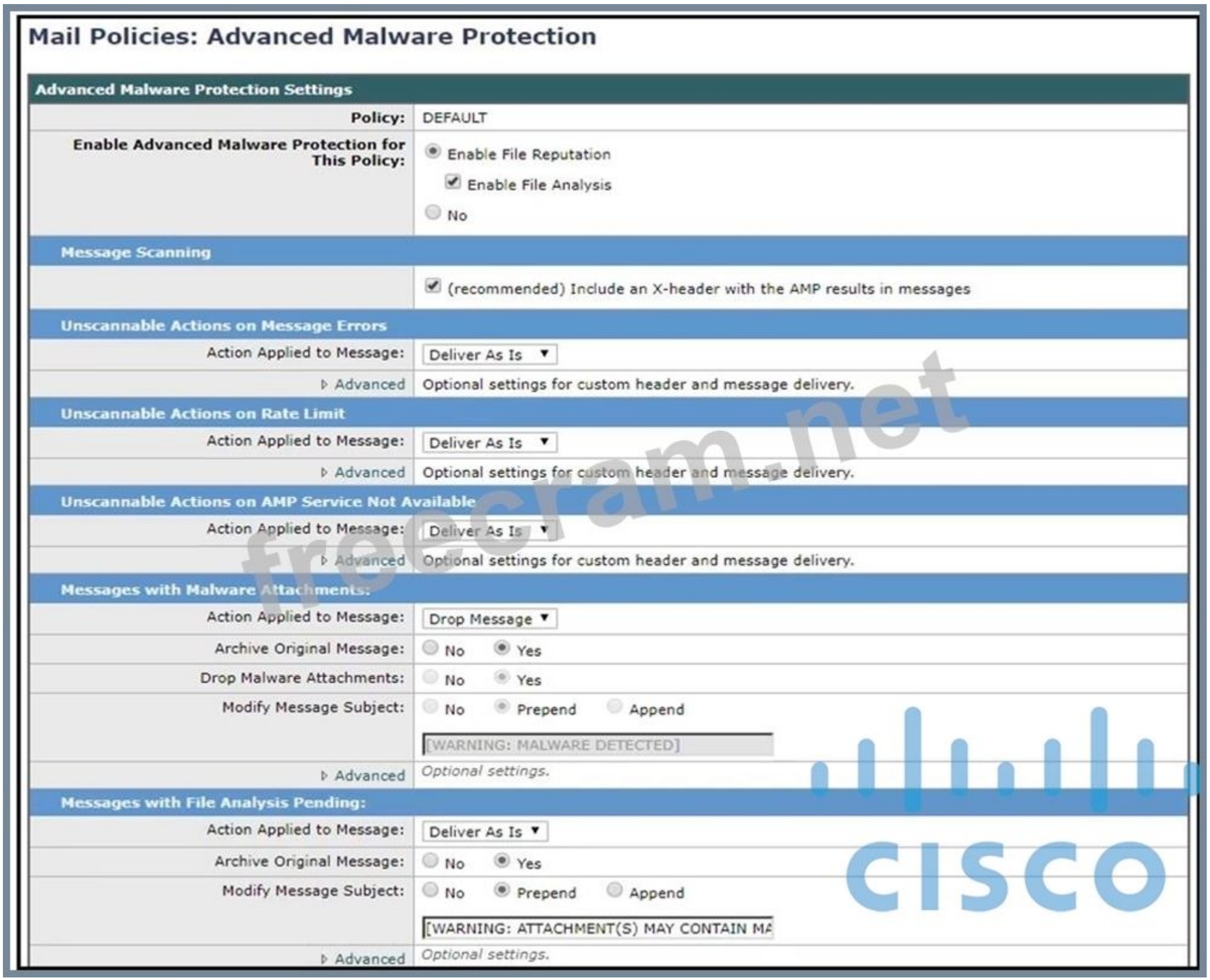
NEW QUESTION: 36
What is a capability of content filters?
A. to apply rules before message filters
B. to scan incoming or outgoing messages
C. to review messages based on email subject
D. to perform antispam scanning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
A network administrator enabled McAfee antivirus scanning on a Cisco Secure Email Gateway and configured the virus scanning action of " scan for viruses only " If the scanner finds a virus in an attachment for an incoming email, what action will be applied to this message?

A. The email and attachment are forwarded to the network administrator.
B. No repair is attempted, and the attachment is either dropped or delivered
C. The attachment is dropped and replaced with a " Removed Attachment " file
D. The system will attempt to repair the attachment
Answer: (SHOW ANSWER)
If the McAfee antivirus scanning is enabled on the Cisco Secure Email Gateway and the virus scanning action is set to "scan for viruses only", then no repair is attempted, and the attachment is either dropped or delivered based on the antiv irus policy settings. The administrator can choose to drop or deliver the infected attachment by selecting the appropriate action in the antivirus policy. References : [Cisco Secure Email Gateway Administrator Guide - Configuring McAfee Antivirus Scanning]

NEW QUESTION: 38
An engineer tries to implement phishing simulations 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 simulations to bypass antispam scanning? (Choose two.) An engineer tries to implement phishing simulations 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 simulations to bypass antispam scanning? (Choose two.)
A. domains
B. spf check
C. A, B
D. receivers
E. senders
F. reputation score
Answer: (SHOW ANSWER)

NEW QUESTION: 39



Refer to the exhibit. How should this configuration be modified to stop delivering Zero Day malware attacks?

A. Change Unscannable Action from Deliver As Is to Quarantine.

B. Change File Analysis Pending action from Deliver As Is to Quarantine.

C. Configure mailbox auto-remediation.

D. Apply Prepend on Modify Message Subject under Malware Attachments.

Answer: (SHOW ANSWER)

Overview of File Reputation Filtering and File Analysis:

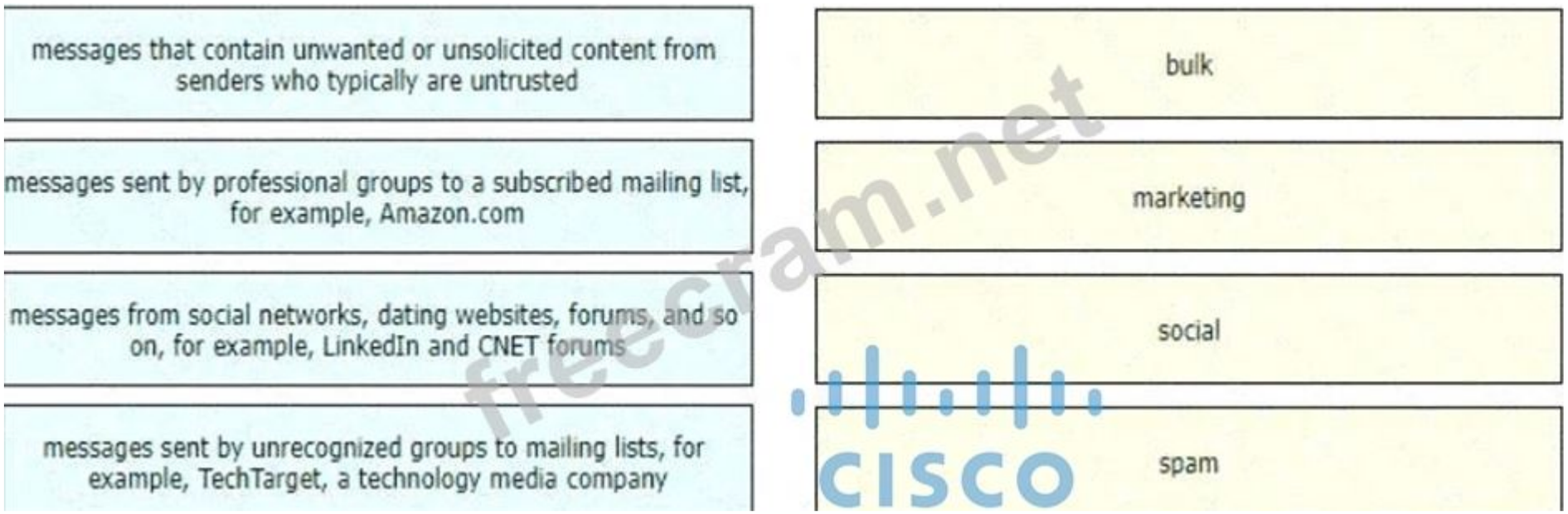
Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:
-Obtaining the reputation of known files.
-Analyzing behavior of certain files that are not yet known to the reputation service.
-Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.
-This feature is available for incoming messages and outgoing messages.
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_010000.html?bookSearch=true

NEW QUESTION: 40

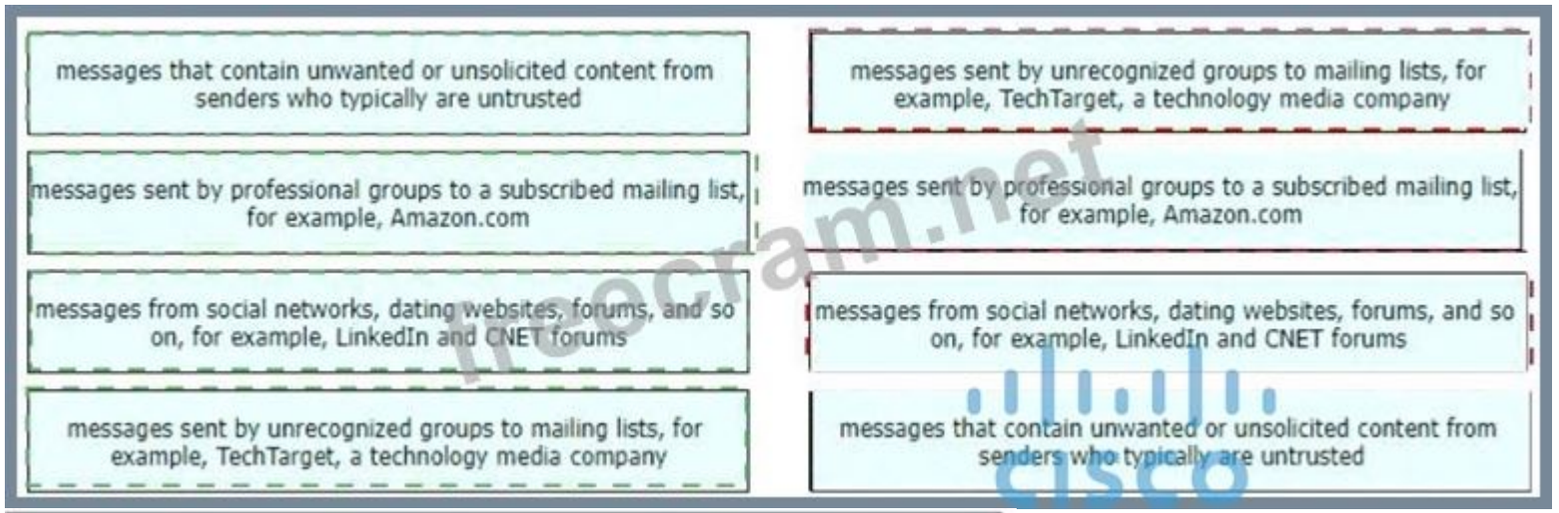
Which two features of Cisco Email Security are added to a Sender Group to protect an organization against email threats? (Choose two.)

A. NetFlow
B. geolocation-based filtering
C. heuristic-based filtering
D. senderbase reputation filtering
E. content disarm and reconstruction
Answer: (SHOW ANSWER)
Geolocation-based filtering and senderbase reputation filtering are two features of Cisco Email Security that can be added to a Sender Group to protect an organization against email threats. Geolocation-based filtering allows Cisco ESA to accept or reject connections from email servers based on their geographic location, such as country or continent. Senderbase reputation filtering allows Cisco ESA to reject or throttle connections from email servers based on their reputation score, which is calculated by Talos using sensor information from various sources.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 5-4 and page 6-2.

NEW QUESTION: 41
Drag and drop the graymail descriptions from the left onto the verdict categories they belong to on the right.



Answer:



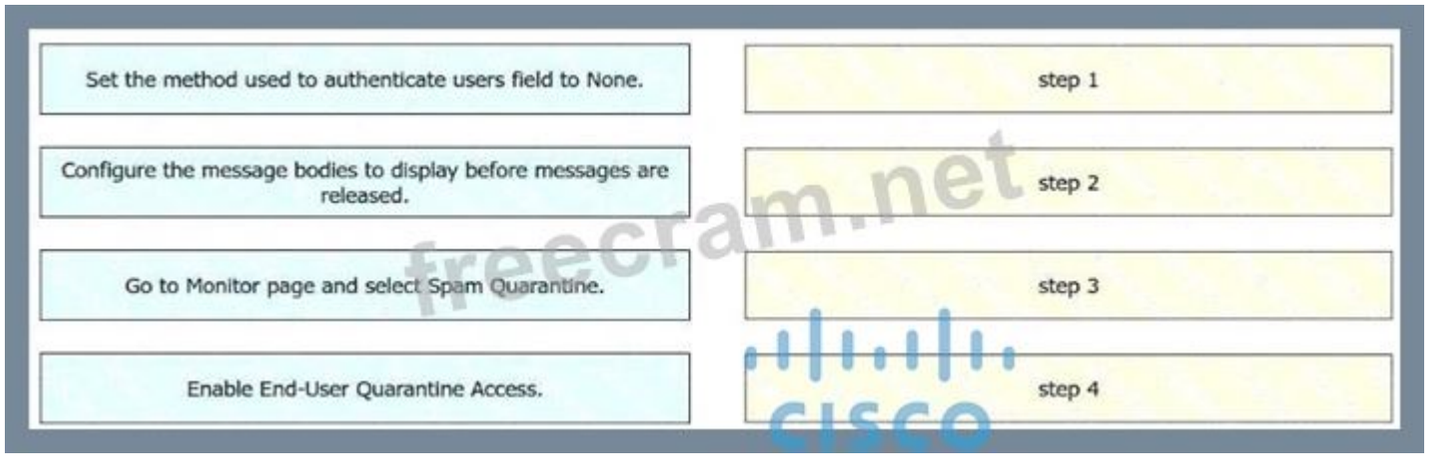
NEW QUESTION: 42
Which content filter condition checks to see if the " From: header " in the message is similar to any of the users in the content dictionary?
A. Forged Email Detection
B. SPF Verification
C. Subject Header
D. Duplicate Boundaries Verification
Answer: (SHOW ANSWER)
The content filter condition that checks to see if the "From: header" in the message is similar to any of the users in the content dictionary is Forged Email Detection. This condition compares the sender's name or email address with a list of names or email addresses in a content dictionary and triggers an action if they match or are similar. References : [Cisco Secure Email Gateway Administrator Guide - Forged Email Detection]

NEW QUESTION: 43
A network engineer must tighten up the SPAM control policy of an organization due to a recent SPAM attack.
In which scenario does enabling regional scanning improve security for this organization?
A. when most of the received spam comes from a specific country

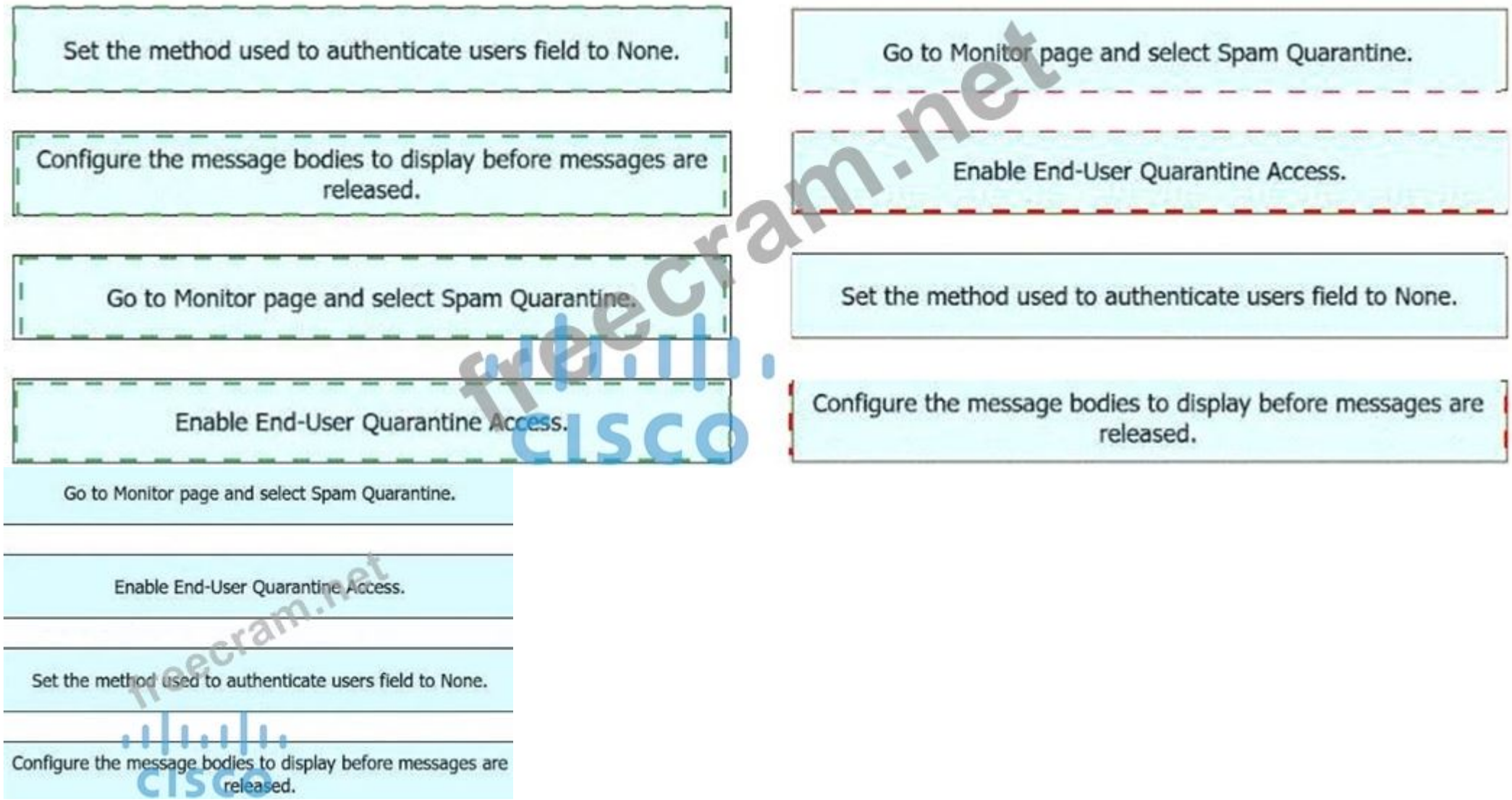
B. when most of the received spam originates outside of the U.S.
C. when most of the received email originates outside of the U.S.
D. when most of the received email originates from a specific region
Answer: (SHOW ANSWER)
Enabling regional scanning improves security for this organization when most of the received email originates from a specific region. Regional scanning is a feature that allows Cisco ESA to apply different spam thresholds and actions based on the geographic region of the sender's IP address, using a database of IP addresses and regions.
To enable regional scanning on Cisco ESA, the administrator can follow these steps:
* Select Security Services > IronPort Anti-Spam and click Edit Settings.
* Under Regional Scanning, select Enable Regional Scanning.
* Click Submit.
* Select Security Services > IronPort Anti-Spam > Regional Settings and click Add Region.
* Choose a region from the drop-down menu, such as Asia Pacific.
* Enter a spam threshold and an action for that region, such as 80 and Drop.
* Click Submit.

NEW QUESTION: 44
Which type of DNS record would contain the following line, which references the DKIM public key per RFC 6376?
v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A2362BECE40658267045694328 3BE
A. CNAME
B. AAAA
C. TXT
D. PTR
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 45
An engineer must provide user access to the spam quarantine on a Cisco Secure Email Gateway. Users must be able to access the spam quarantine without additional authentication by using links. The users must be able to preview a spam message from within the Spam Quarantine section without restoring the message. Drag and drop the actions from the left into sequence on the right to meet the requirements.



Answer:



NEW QUESTION: 46

An organization is enforcing TLS with an external party. The external business employs its own internal CA so the Secure Email Gateway cannot verify the TLS connection. Which action must an engineer take for the Cisco Secure Email Gateway to trust the connection?

A. Modify Destination Controls and set TLS Support to Required for all external and internal destinations.

B. Edit Destination Controls and add the external party domain to the Destination Control Table as trusted.

C. Enable a custom list on the Network > Certificates page and upload the certificates for the trusted authorities.

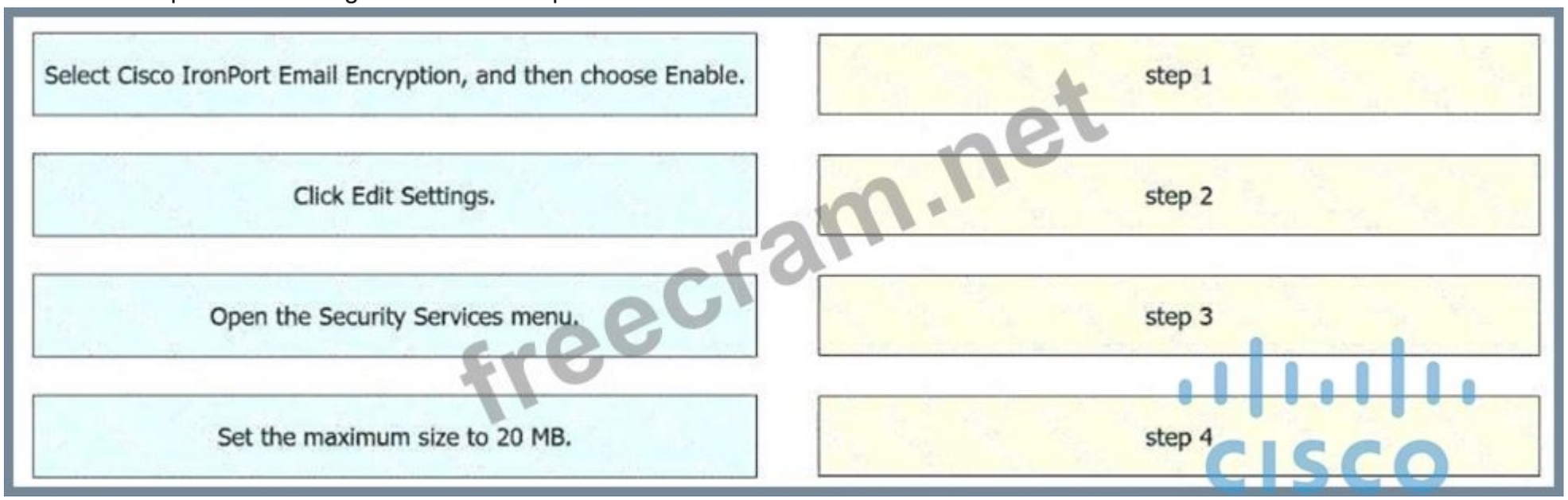
D. Choose Add Certificate on the Network > Certificates page and create a self-signed certificate.
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which 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: (SHOW ANSWER)
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:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[] > NEW
Enter filter script. Enter ' . ' on its own line to end.
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
quarantine(" large_spam ");
log-entry(" *****This is a large message with no attachments***** ");
}
1 filters added.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213940-esa-using- a- message-filter-to-take-act.html

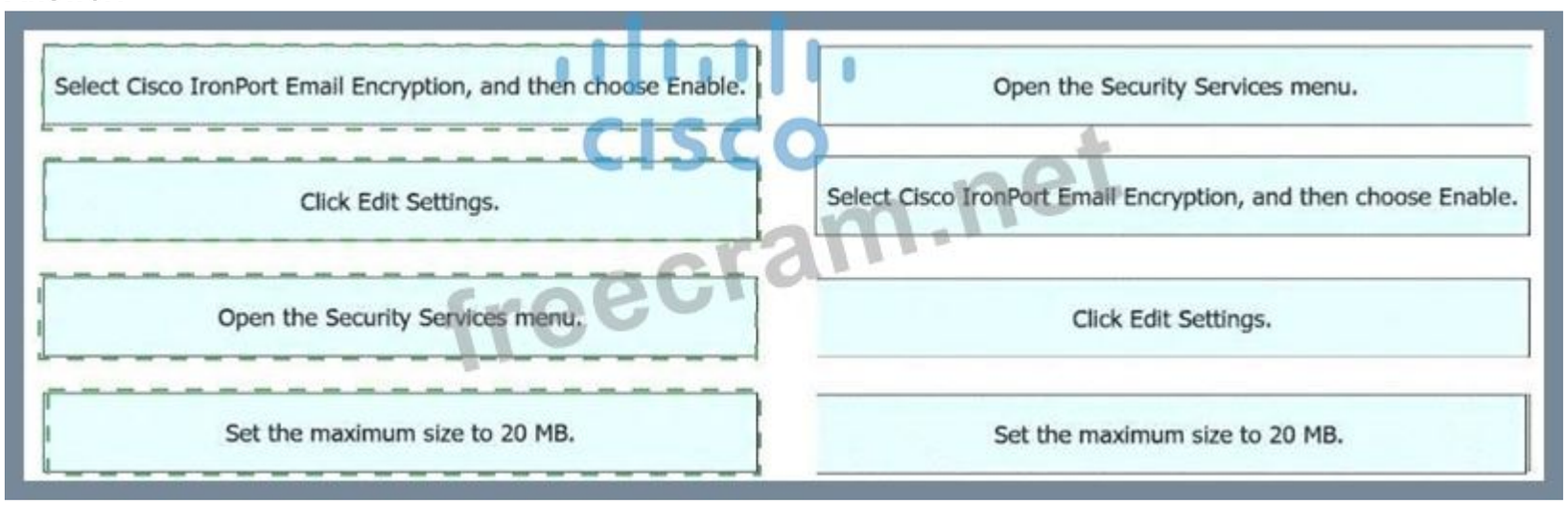
NEW QUESTION: 48
An engineer must configure a local spam quarantine in Cisco Secure Email Gateway These configurations were already performed: *Enable the Anti-Spam feature and configure the quarantine settings *Specify the disk space to allocate to the spam quarantine.
Which two actions must be taken to complete the configuration? (Choose two.)
A. Configure a mail policy.
B. Enable Outbreak Filters.
C. Activate Outgoing Content Filters.

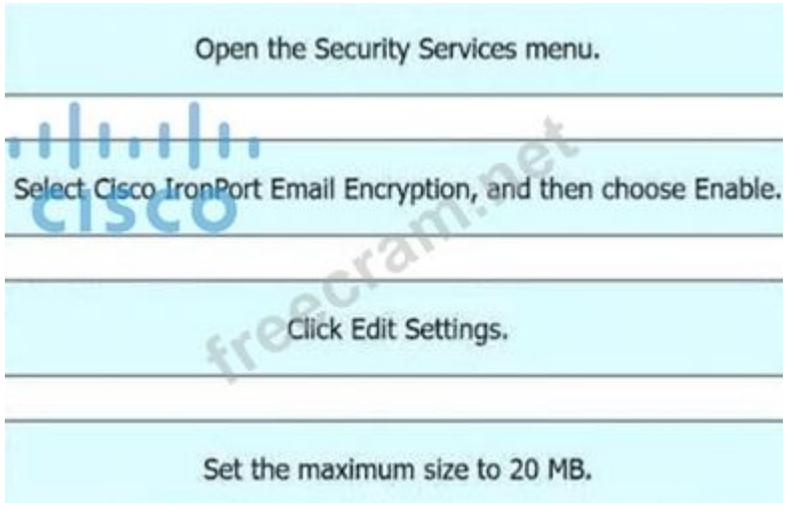
D. Allow browser access
E. Set the quarantine threshold to 3
Answer: (SHOW ANSWER)

NEW QUESTION: 49
An engineer must enable encryption on a Cisco Secure Email Gateway. The maximum size of each message must be 20 MB. Drag and drop the actions from the left into sequence on the right to meet the requirement.



Answer:





NEW QUESTION: 50

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?

A. Enable the external Spam Quarantine and enter the IP address and port for the Secure Email and Web Manager

B. Enable the Spam Quarantine and leave the default settings unchanged.

C. Enable End-User Quarantine Access and point to an LDAP server for authentication.

D. Enable the Spam Quarantine and specify port 80 for HTTP and port 443 for HTTPS

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 51

Which process is skipped when an email is received from safedomain.com, which is on the safelist?

A. message filter

B. antivirus scanning

C. outbreak filter

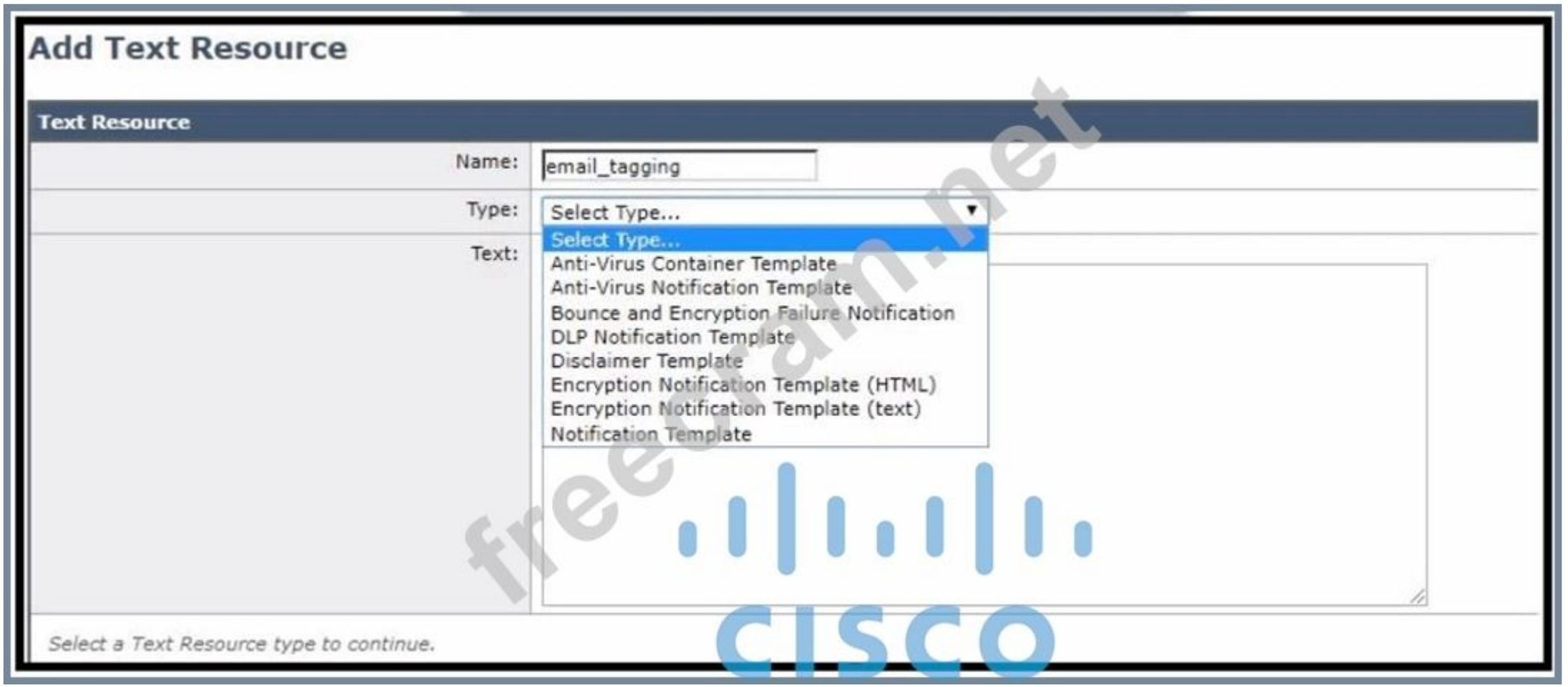
D. antispam scanning

Answer: (SHOW ANSWER)

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.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-13.

NEW QUESTION: 52
Refer to the exhibit.



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?

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: (SHOW ANSWER)

According to the [Cisco Secure Email User Guide], you can create a text resource of type Dis claimer 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:

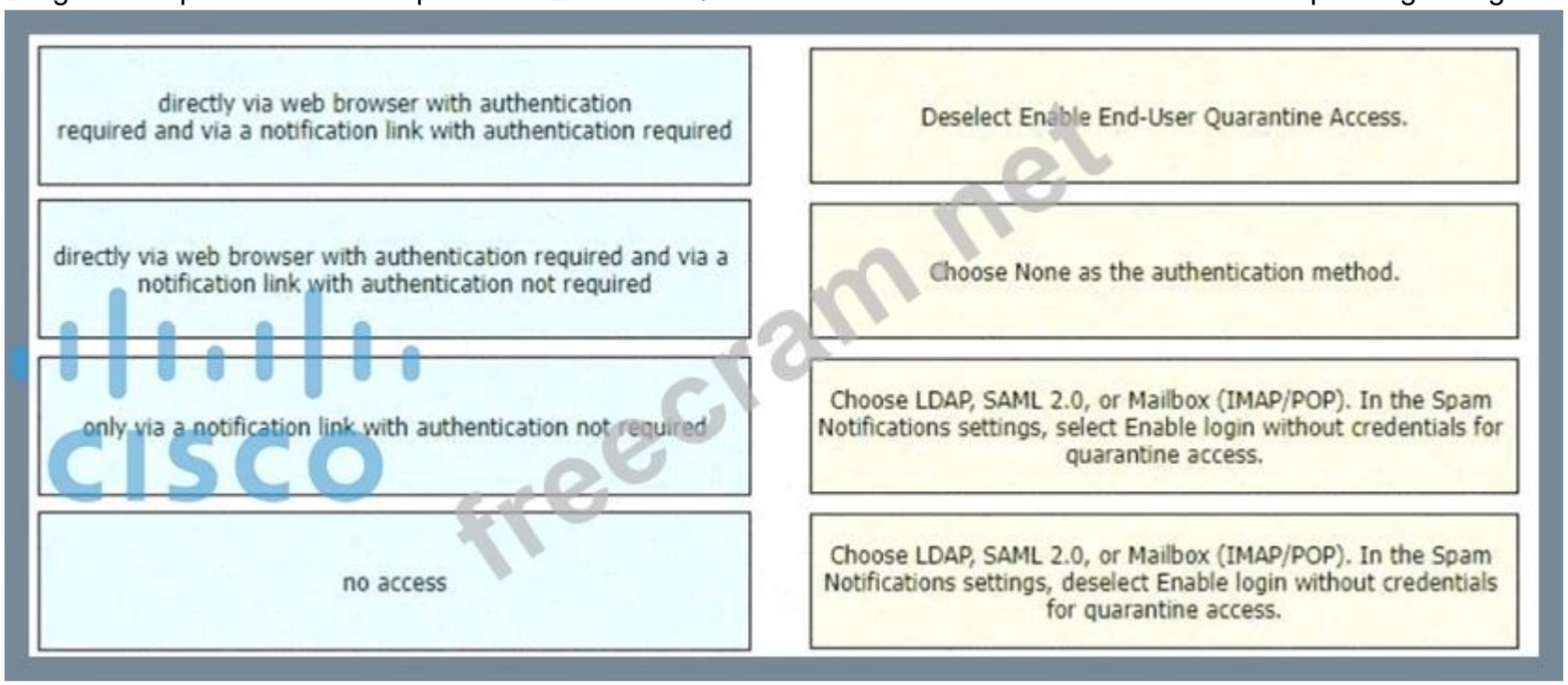
* A. Creating a text resource type of Disclaimer Template and pasting the HTML code into the text box without changing to code view will not work, as the HTML code will be treated as plain text and not rendered properly[1 , p. 15].

* C. Creating a text resource ty pe 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].

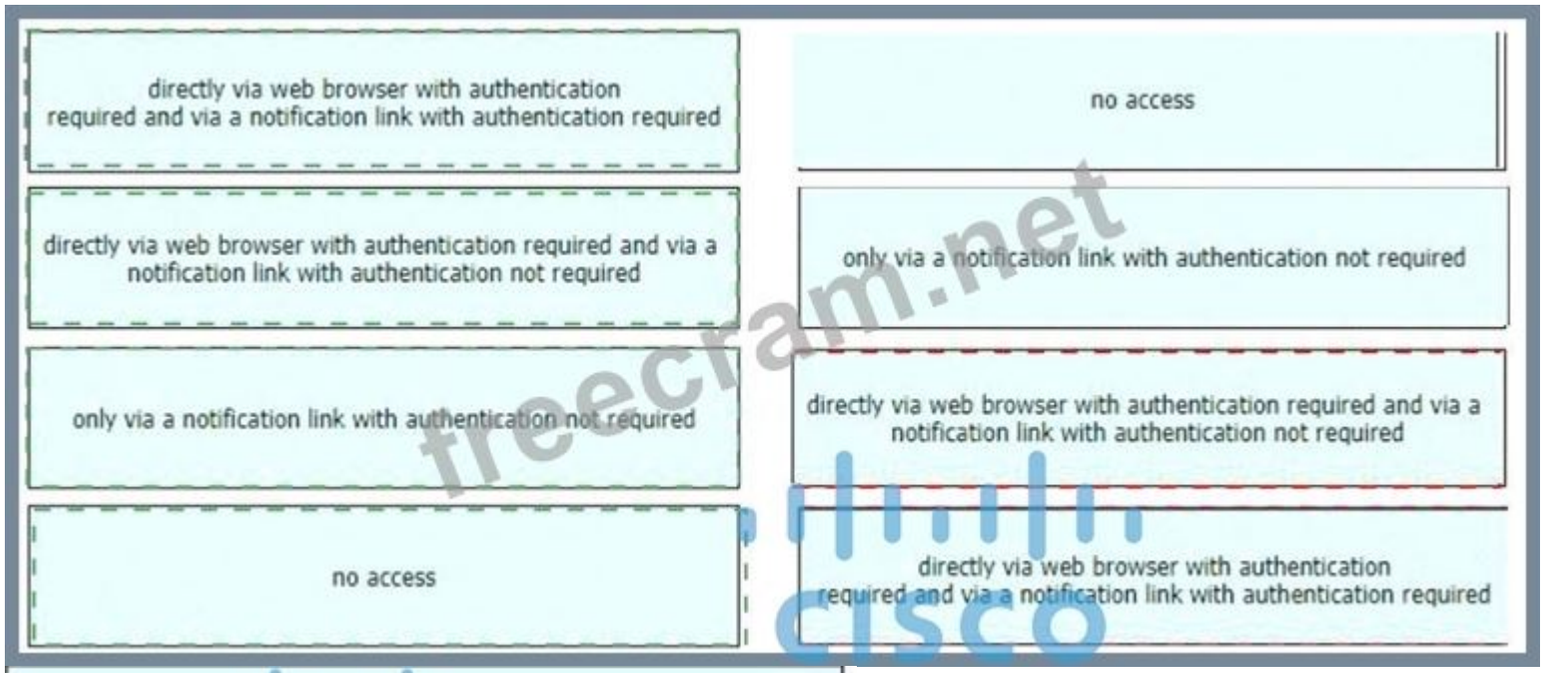
* D. Creating a text resource type of No tification Template and changing to code view to paste the HTML code into the text box will not work, as Notification Templates are used for sending notifications to senders or recipients, not for modifying the email body[1 , p. 17].

NEW QUESTION: 53
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: (SHOW ANSWER)
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.
References: User Guide for AsyncOS 15.0 f or Cisco Secure Email Gateway , page 10-2.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa- 00.
html (configuration summary)

NEW QUESTION: 54
Drag and drop authentication options for End-User Quarantine Access from the left onto the corresponding configuration steps on the right.



Answer:



NEW QUESTION: 55

Which two are configured in the DMARC verification profile? (Choose two.)

A. name of the verification profile

B. minimum number of signatures to verify

C. ESA listeners to use the verification profile

D. message action into an incoming or outgoing content filter

E. message action to take when the policy is reject/quarantine

Answer: (SHOW ANSWER)

A DMARC verification profile is a list of parameters that the mail flow policies of the appliance use for verifying DMARC. The name of the verification profile identifies the profile and allows you to apply it to different mail flow policies. The message action to take when the policy is reject/quarantine determines how the appliance handles messages that fail DMARC verification based on the sender's DMARC policy.
References: User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment)
, Chapter: Email Authentication, Section: Configuring DMARC Verification 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_010101.html#task_1231917

NEW QUESTION: 56
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' that has yet to be create d.
Which mail policy should be created to accomplish this task?
A. Outgoing Mail Policy
B. Preliminary Mail Policy
C. Incoming Mail Flow Policy
D. Outgoing Mail Flow Policy
Answer: (SHOW ANSWER)
Outgoing Mail Policy is a mail policy that should be created to accomplish this task. Outgoing Mail Policy is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.
To create an Outgoing Mail Policy named 'Sales' and assign a DLP policy to it, the administrator can follow these steps:
* Select Mail Policies > Outgoing Mail Policies and click Add Policy.
* Enter 'Sales' as the policy name and click Submit.
* Select 'Sales' from the list of policies and click Edit Settings.
* Under Data Loss Prevention, select Enable Data Loss Prevention Scanning and choose the DLP policy from the drop-down menu.
* Click Submit.
The other options are not valid mail policies to accomplish this task, because they do not apply to outgoing messages or DLP scanning.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2 and page 9-4.

NEW QUESTION: 57
An engineer deploys a Cisco Secure Email Gateway appliance with default settings in an organization that permits only standard H feature does not work. Which additional action resolves the issue?
A. Configure the outbound firewall rule to permit traffic on port 8081
B. Enable the Use HTTP option under Advanced Settings for File Reputation.
C. Enable the Use SSL option under Advanced Settings for File Reputation.
D. Configure the outbound firewall rule to permit traffic on port 3237
E. TP/HTTPS ports outbound and notices that the AMP file reputation
Answer: (SHOW ANSWER)
Configuring the outbound firewall rule to permit traffic on port 3237 is the additional action that resolves the issue. AMP file reputation is a feature that allows Cisco ESA to check files attached to messages against a cloud-based database of known malicious files and apply appropriate actions, such as block, deliver, or quarantine.
By default, AMP file reputation uses TCP port 3237 to communicate with the cloud-based database. If this port is blocked by a firewall, AMP file reputation will not work properly.

To resolve this issue, the administrator can configure the outbound firewall rule to permit traffic on port 3237 from Cisco ESA.
The other options are not valid actions to resolve the issue, because they do not affect the port used by AMP file reputation.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 7-5 and page 7-6.

NEW QUESTION: 58
A content dictionary was created for use with Forged Email Detection. Proper data that pertains to the CEO Example CEO: <ceo@example com> must be entered. What must be added to the dictionary to accomplish this goal?
A. example.com
B. Example CEO
C. ceo
D. ceo@example com
Answer: (SHOW ANSWER)
ceo@example.com is the data that must be added to the dictionary to accomplish this goal. A content dictionary is a list of values that can be used as a condition in a content filter or a message filter. Forged Email Detection is a feature that allows Cisco ESA to detect and prevent email spoofing attacks, where the sender's address or domain is forged to appear as someone else, such as the CEO of the organization.
To create a content dictionary for use with Forged Email Detection on Cisco ESA, the administrator can follow these steps:
Select Mail Policies > Content Dictionaries and click Add Dictionary.
Enter a name and description for the content dictionary, such as CEO Email.
Under Dictionary Values, click Add Value.
Enter the email address of the CEO, such as ceo@example.com.
Click Submit.

NEW QUESTION: 59
An admin istrator 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 p olicy 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 exte rnal quarantine.
Answer: (SHOW ANSWER)
Disabling the Local Spam Quarantine to Activate the External Quarantine If you were using a local spam quarantine before enabling an external spam quarantine, you must disable the local quarantine in order to send messages to the external quarantine.
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_0101010.html?bookSearch=true#con_1172419

NEW QUESTION: 60
Which 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: (SHOW ANSWER)

Spam Quarantine Alias Consolidation Query is a type of query that must be configured when setting up the Spam Quarantine while merging notifications on Cisco ESA. This query allows Cisco ESA to consolidate multiple email addresses that belong to the same end user into one entry in the Spam Quarantine, and send only one notification email to that end user with all the quarantined messages for all their email addresses.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-10.

NEW QUESTION: 61

An engineer must configure a policy quarantine in Cisco Secure Email Gateway. The retention time must be 7 days and user@cisco.com must have access to the quarantine. Drag and drop the actions from the left into the sequence on the right to meet the requirements.

Answer:

Set the retention time to 7 days.

Give user@cisco.com access to the quarantine.

Submit and commit the changes.

Configure the Policy, Virus, and Outbreak Quarantines settings.

Add a new policy quarantine.

Configure the Policy, Virus, and Outbreak Quarantines settings.

Add a new policy quarantine.

Set the retention time to 7 days.

Give user@cisco.com access to the quarantine.

Submit and commit the changes.

Configure the Policy, Virus, and Outbreak Quarantines settings.

Add a new policy quarantine.

Set the retention time to 7 days.

Give user@cisco.com access to the quarantine.

Submit and commit the changes.

freecram.net

NEW QUESTION: 62
An engineer must ensure that email sent from is not sent to the spam quarantine on a Cisco Secure Email Gateway. What must be configured on the Secure Email Gateway?
A. URL filtering
B. content filter
C. safelist
D. S/MIME
Answer: (SHOW ANSWER)

NEW QUESTION: 63
A network engineer is integrating Cisco Secure Email Gateway with Cisco SecureX. Which two actions must be taken before registering Cisco Secure Email Gateway with Cisco SecureX? (Choose two.)
A. Run the cloudserviceconflg command in SecureX
B. Open TCP port 443 on the firewall.
C. Run the threatresponseconflg command in SecureX
D. Create an admin account in SecureX
E. Open TCP port 22 on the firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 64
What is the function of authenticating SMTP sessions using client certificates?
A. Users must configure a mail client to send messages through a secure SSL connection and accept a server certificate from the appliance.
B. The Secure Email Gateway requests a client certificate from a user ' s mail client during connection to the appliance.
C. If the certificate is valid, the Secure Email Gateway allows an SMTP connection from the mail client over TLS.
D. If the Secure Email Gateway is configured to require users to provide a certificate when sending mail, no exceptions are allowed for any users.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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?
A. Accept
B. Delay
C. Relay
D. Reject
Answer: (SHOW ANSWER)

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.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 6-2 and page 6-3.

NEW QUESTION: 66
What validates users via LDAP during login to end-user quarantine?
A. end-user authentication query
B. LDAP authentication query
C. alias consolidation query
D. external authentication query
Answer: (SHOW ANSWER)

NEW QUESTION: 67
A network administrator notices that there are a high number of queries to the LDAP server. The mail logs show an entry "550 Too many invalid recipients | Connection closed by foreign host." Which feature must be used to address this?
A. DHAP
B. SBRS
C. LDAP
D. SMTP
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0
/b_ESA_Admi n_Guide_12_0_chapter_011010.html
DHAP (Directory Harvest Attack Prevention) is a feature that must be used to address this issue. DHAP is a mechanism that allows Cisco ESA to prevent directory harvest attacks, which are attempts by spammers or hackers to obtain valid email addresses from an LDAP server by sending messages with random or guessed recipients and checking for bounce messages.
To enable DHAP on Cisco ESA, the network administrator can follow these steps:
Select Network > Listeners and click Edit Settings for the listener that receives incoming messages.
Under SMTP Authentication Settings, select Enable Directory Harvest Attack Prevention.
Enter a value for Maximum Invalid Recipients per Hour, which is the number of invalid recipients that triggers DHAP.
Enter a value for Block Sender for (hours), which is the duration that Cisco ESA blocks messages from senders who exceed the maximum invalid recipients per hour.
Click Submit.

NEW QUESTION: 68
An engineer must add the user1@cisco.co m with an IP address of 10.1.1.13 to a safelist in Cisco Secure Email Gateway. Which two safelist syntaxes must be configured to meet the requirement? (Choose two.)
A. [10.1.1.0/24]
B. [10.1.1.16/30]
C. [10.1.1.13/30]
D. user1@ [10.1.1.13]
Answer: (SHOW ANSWER)

NEW QUESTION: 69
A trusted partner of an organization recently experienced a new campaign that was leveraging JavaScript attachments to trick users into executing malware. As a result, they created a local policy to deny messages with JavaScript attachments. Which action should the administrator of the organization take to ensure encrypted communications are delivered to the intended partner recipient?
A. Insert the X-PostX-Use-Script' header with a value of false to the encrypted messages
B. Select JavaScript-free' option within the Cisco Secure Email Encryption Service Add-in
C. Create an outgoing content filter and add the Encrypt and Deliver Nov/ action with Use-Script option deselected
D. Create a new encryption profile and deselect the 'Use-Script' envelope settings option.
Answer: (SHOW ANSWER)
According to the User Guide for Cisco Secure Email Encryption Service Add-In 1, the 'Use-Script' option allows you to use JavaScript in the encrypted message envelope. This option is enabled by default, but you can disable it if you want to send encrypted messages to recipients who have security policies that block JavaScript attachments[2, p. 14].
The other options are not valid because:
A) Inserting the X-PostX-Use-Script header with a value of false to the encrypted messages is not a supported feature of the Cisco Secure Email Encryption Service Add-in1.
B) Selecting JavaScript-free option within the Cisco Secure Email Encryption Service Add-in is not a valid option. The add-in does not have such an option1.
C) Creating an outgoing content filter and adding the Encrypt and Deliver Nov/ action with Use-Script option deselected is not possible. The Encrypt and Deliver Nov/ action does not have a Use-Script option[2, p. 13].

NEW QUESTION: 70
An engineer must share threat reporting information from Cisco Secure Email Gateway to Cisco SecureX.
Which setting must be enabled in Secure Email Gateway?

A. Security Services Exchange
B. Cloud Service Settings
C. System Monitor
D. SNMP
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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?

A. The sender is included in an ISP blocklist
B. Administrative access is required to create a safelist.
C. The sender didn ' t mark the message as urgent
D. End-user safelists apply to antispam engines only.
Answer: (SHOW ANSWER)
The reason why the CEO did not receive an important message expected from a trusted sender after adding them to a safelist is beca use 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 exem pt 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. References = User Guide for AsyncOS
12.0 for Cisco Email Security Appliances - GD (General Deployment) - Safelists and Blocklists [Cisco Secure Email Gateway] - Cisco

NEW QUESTION: 72
Which global setting is configured under Cisco ESA Scan Behavior?
A. minimum attachment size to scan
B. attachment scanning timeout
C. actions for unscannable messages due to attachment type
D. minimum depth of attachment recursion to scan
Answer: (SHOW ANSWER)
The global setting that is configured under Cisco ESA Scan Behavior is the actions for unscannable messages due to attachment type. This setting allows the administrator to specify what action to take when a message contains an attachment that cannot be scanned by the appliance, such as encrypted or password-protected files. The possible actions are:
* Deliver - Deliver the message normally.
* Drop - Drop the message silently without notifying the sender or recipient.
* Quarantine - Quarantine the message in a specified policy quarantine.
* Bounce - Bounce the message back to the sender with a specified reason.
Reference:
Scan Behavior
Reference: https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scan-behavior- impact-on-av/td-p/3923243

NEW QUESTION: 73
What are two prerequisites for implementing undesirable URL protection in Cisco ESA? (Choose two.)
A. Enable outbreak filters.
B. Enable email relay.
C. Enable antispam scanning.
D. Enable port bouncing.
E. Enable antivirus scanning.
Answer: (SHOW ANSWER)
Undesirable URL protection is a feature that allows Cisco ESA to detect and block messages that contain URLs that lead to malicious or unwanted websites, such as phishing, malware, or adult content sites. To enable this feature, outbreak filters and antispam scanning must be enabled on Cisco ESA.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-17.

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_01111.html

NEW QUESTION: 74
Which components are required when encrypting SMTP with TLS on a Cisco Secure Email Gateway appliance when the sender requires TLS verification?
A. DER certificate and matching public key from a CA
B. self-signed certificate in PKCS#7 format
C. X. 509 certificate and matching private key from a CA
D. self-signed certificate in PKCS#12 format
Answer: C (LEAVE A REPLY)
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. References : [Cisco Secure Email Gatew ay Administrator Guide - Configuring TLS]

NEW QUESTION: 75
Which two query types are available when an LDAP profile is configured? (Choose two.)
A. proxy consolidation
B. user
C. recursive
D. group
E. routing
Answer: (SHOW ANSWER)
User and routing are two query types that are available when an LDAP profile is configured on Cisco ESA.
User queries are used to validate end-user credentials, such as for Spam Quarantine End-User Authentication or SMTP Authentication. Routing queries are used to determine the destination mail server for a recipient, such as for Mail Flow Policies or Delivery Methods.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-7.

NEW QUESTION: 76

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Not Available	Disabled	Retention Time: Virus: 1 day	Not Available	

Refer to the exhibit. How does a Cisco Secure Email Gateway handle an email that is identified both as spam positive and outbreak positive by outbreak filters?
A. The email is sent only to the spam quarantine.
B. The email is sent to outbreak quarantine and is rescanned for spam before being released.
C. The email is sent only to the outbreak quarantine.
D. The email is sent to spam quarantine and outbreak quarantine.

Answer: (SHOW ANSWER)

NEW QUESTION: 77
An engineer must modify the altsrchost table on a Cisco Secure Email Gateway Messages destined for a domain named @cisco.com must be mapped to NewInterface with an IP address of 10.10.10.1. What must be added to the table?
A. NewInterface @cisco.com
B. @cisco.com NewInterface
C. cisco.com NewInterface
D. Cisco com 10.10.10.1
Answer: (SHOW ANSWER)

NEW QUESTION: 78
An organization wants to use DMARC to improve its brand reputation by leveraging DNS records.
Which two email authentica tion mechanisms are utilized during this process? (Choose two.)
A. SPF
B. DSTP
C. DKIM
D. TLS
E. PKI
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/products/security/what-is-dmarc.html
SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) are two email authentication mechanisms that are utilized during this process. SPF and DKIM allow the domain owner to publish DNS records that specify the authorized IP addresses or hosts for sending emails from that domain and sign the messages with a cryptographic key to prove their authenticity and integrity.
DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication standard that builds on SPF and DKIM and allows the domain owner to publish DNS records that specify how receivers should handle messages that fail SPF or DKIM verification, such as reject, quarantine, or none, and how to report back the results of DMARC validation.
The other options are not valid email authentication mechanisms that are utilized during this process, because they are not part of DMARC standard.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 11-2 and page 11-3.

NEW QUESTION: 79
Which feature must be activated on a Cisco Secure Email Gateway to combat backscatter?
A. Graymail Detection
B. Bounce Verification

C. Forged Email Detection
D. Bounce Profile
Answer: (SHOW ANSWER)
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. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Bounce Verification]

NEW QUESTION: 80
Which setting affects the aggressiveness of spam detection?
A. protection level
B. spam threshold
C. spam timeout
D. maximum depth of recursion scan
Answer: (SHOW ANSWER)
Spam threshold is a setting that determines the minimum score that a message must have to be classified as spam by Cisco ESA. The lower the threshold, the more aggressive the spam detection is.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-5.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118220-technote- esa-00.html

NEW QUESTION: 81
Which two Cisco ESA features are used to control email delivery based on the sender? (Choose two.)
A. incoming mail policies
B. spam quarantine
C. outbreak filter
D. safelists
E. blocklists
Answer: (SHOW ANSWER)
Safelists and blocklists are features on Cisco ESA that allow you to control email delivery based on the sender. Safelists are lists of sender addresses or domains that you want to accept or exempt from certain filtering actions. Blocklists are lists of sender addresses o r domains that you want to reject or drop 3 .
References = Securing Email with Cisco Email Security Appliance (SESA) v3.1

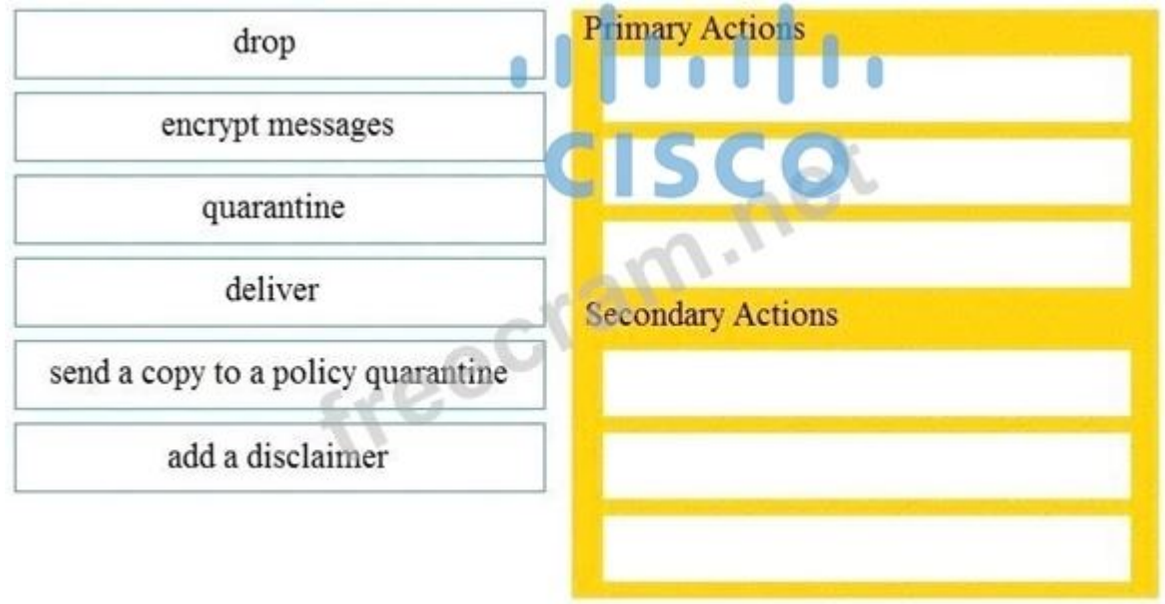
NEW QUESTION: 82
Which two factors must be considered when message filter processing is configured? (Choose two.)
A. message-filter order
B. lateral processing
C. structure of the combined packet
D. mail policies
E. MIME structure of the message
Answer: (SHOW ANSWER)

Message-filter order and MIME structure of the message are two factors that must be considered when message filter processing is configured on Cisco ESA. Message-filter order determines the sequence in which message filters are evaluated and applied to incoming messages, which can affect the final outcome of the filtering process. MIME structure of the message determines how message filters match against different parts of the message, such as headers, body, attachments, etc., which can affect the accuracy and performance of the filtering process.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 3-3 and page 3-5.
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

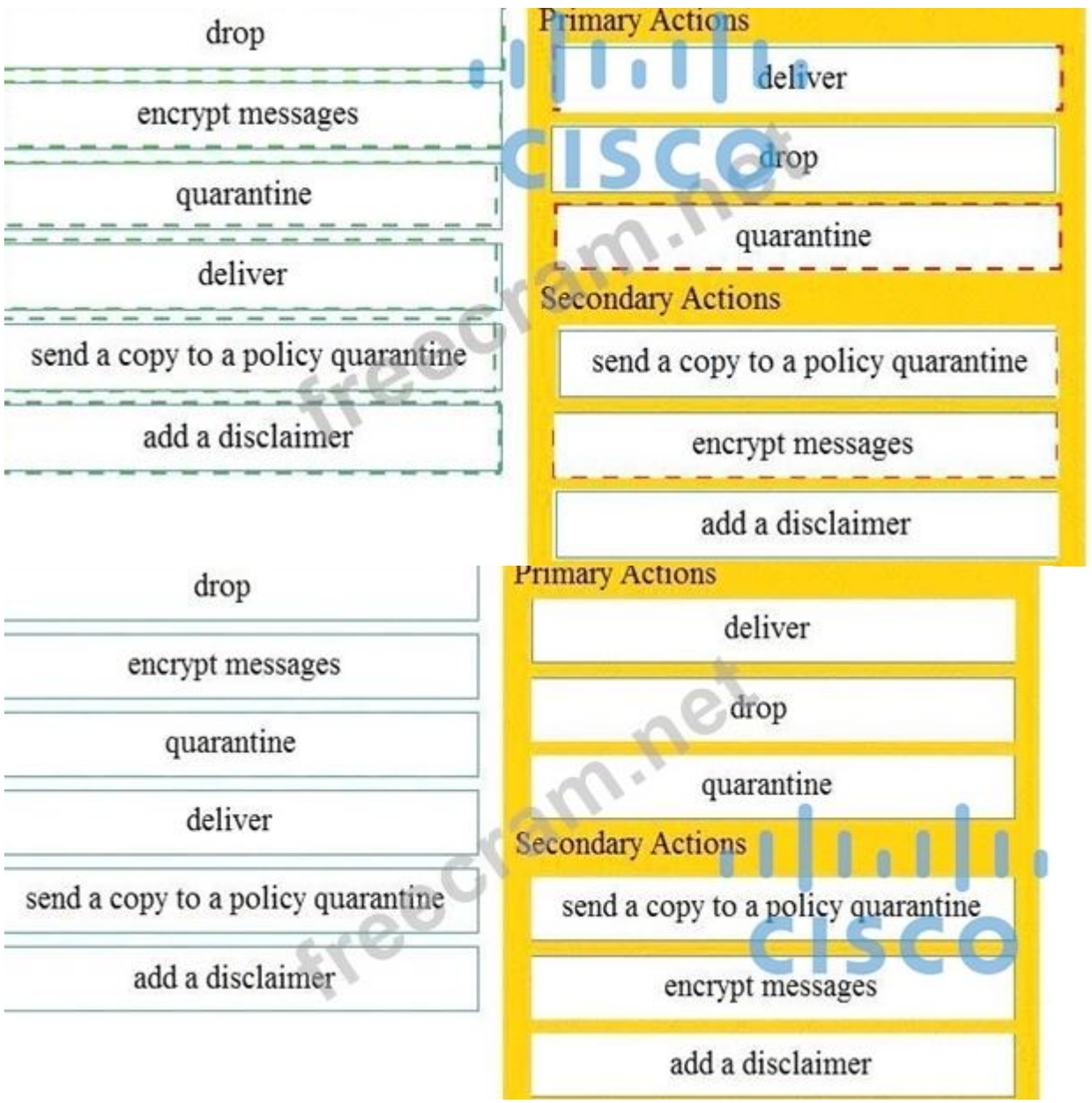
NEW QUESTION: 83
What is the maximum message size that can be configured for encryption on the Cisco ESA?
A. 20 MB
B. 25 MB
C. 15 MB
D. 30 MB
Answer: B (LEAVE A REPLY)
The maximum message size that can be configured for encryption on the Cisco ESA is 25 MB. This is the default value for the Maximum Message Size for Encryption setting in the Encryption Profile. Messages that exceed this size will not be encrypted and will be delivered as normal.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 12-6.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117972-technote- esa-00.html

NEW QUESTION: 84
An engineer must configure Directory Harvest Attack Prevention for SMTP in Cisco Secure Email Gateway.
This error message must be sent when the listener receives more than 50 invalid recipients per hour.
*500 - Too many requests
*Max. Invalid Recipients Per Hour was set to 50 already.
Which two actions must be taken next to set maximum invalid recipients per hour to meet the requirement?
(Choose two.)
A. Implement Max. Recipients Per Hour Text to 500 - Too many requests.
B. Set Max. Recipients Per Hour Text to Too many requests.
C. Configure Max. Recipients Per Hour Code to 500.
D. Create Max. Recipients Per Hour Code to 500.
E. Apply Max. Recipients Per Hour Text to 500 - Too many requests.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Drag and drop the Cisco ESA reactions to a possible DLP from the left onto the correct action types on the right.



Answer:



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_010001.html (message actions)

NEW QUESTION: 86
Refer to the exhibit.

Which SPF record is valid for mycompany.com?
A. v=spf1 a mx ip4:199.209.31.2 -all
B. v=spf1 a mx ip4:10.1.10.23 -all
C. v=spf1 a mx ip4:199.209.31.21 -all
D. v=spf1 a mx ip4:172.16.18.230 -all
Answer: (SHOW ANSWER)
The SPF record for mycompany.com is shown in the exhibit as:
v=spf1 a mx ip4:199.209.31.21 -all
This means that the domain mycompany.com authorizes the following sources to send email on its behalf:
* The A record of mycompany.com, which resolves to 199.209.31.21
* The MX record of mycompany.com, which points to mail.mycompany.com, which also resolves to 199.209.31.21
* The IP address 199.209.31.21
* The -all qualifier means that any other source is not authorized and should be rejected.
Therefore, the correct answer is C.
References:
SPF Record Syntax
Define your SPF record-Basic setup

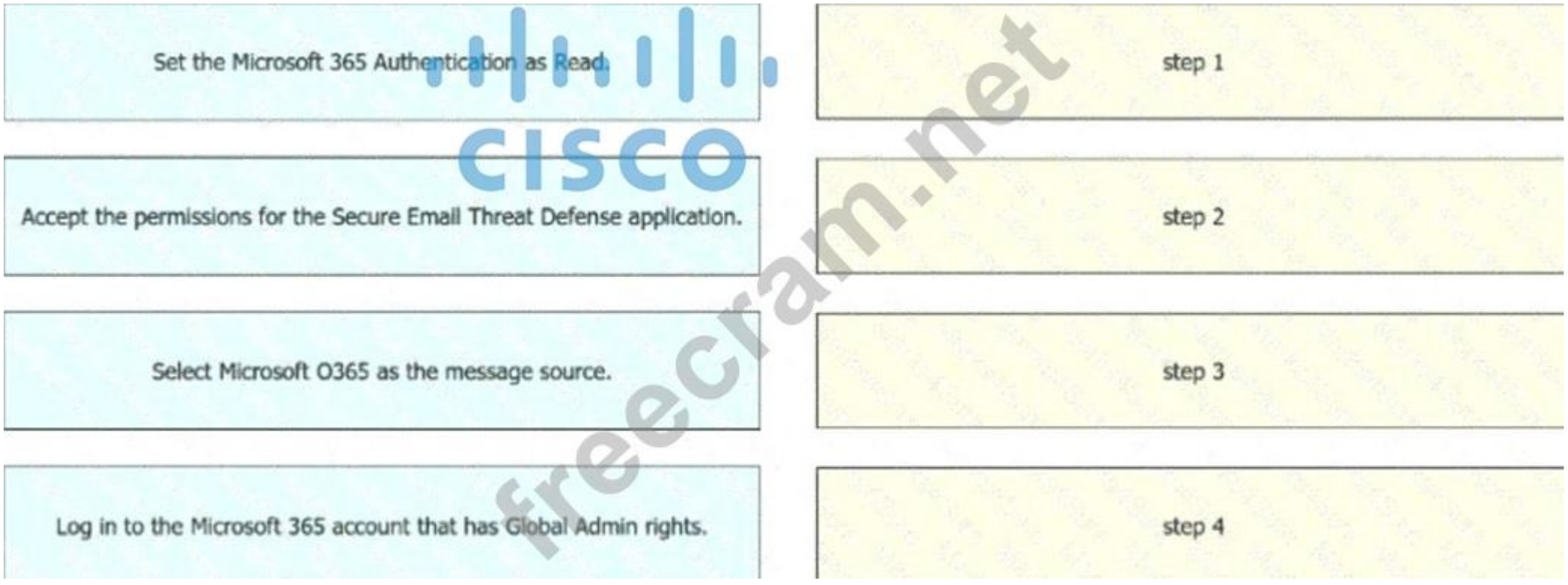
NEW QUESTION: 87
Which of the following two steps are required to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance? (Choose two.)
A. Paste in the Registration Token generated from the Smart Licensing Account
B. Enable the Threat Response service under Network>Cloud Service Settings.
C. Select the correct Threat Response Server based on your region.
D. Paste in the Registration Token generated from the Security Services Exchange.
E. Enable the Security Services Exchange service under Network>Cloud Service Settings
Answer: (SHOW ANSWER)
one of the methods to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance is to use the Threat Response service1. This service allows the appliance to send telemetry data to the SecureX cloud and provide visibility and response capabilities across multiple security products1. To use this service, the administrator needs to perform the following steps1:
Enable the Threat Response service: The administrator needs to go to Network > Cloud Service Settings and enable the Threat Response service. This will generate a registration token that can be used to register the appliance with SecureX1.
Select the correct Threat Response Server: The administrator needs to select the appropriate Threat Response server based on the region where the appliance is located. The available regions are North America, Europe, and Asia Pacific1.

NEW QUESTION: 88
An engineer is configuring an SMTP authentication profile on a Cisco ESA which requires certificate verification.
Which section must be configured to accomplish this goal?
A. Mail Flow Policies
B. Sending Profiles
C. Outgoing Mail Policies
D. Verification Profiles
Answer: (SHOW ANSWER)

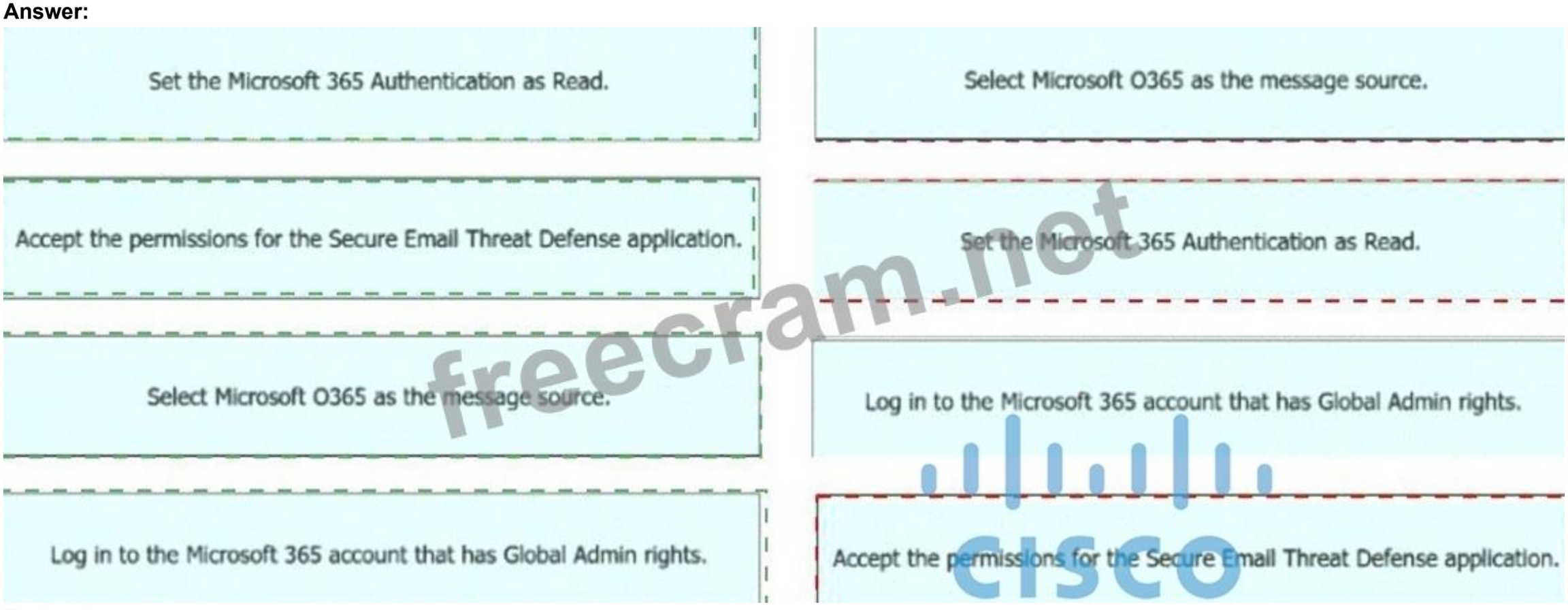
NEW QUESTION: 89
Which two action types are performed by Cisco ESA message filters? (Choose two.)
A. non-final actions
B. filter actions
C. discard actions
D. final actions
E. quarantine actions
Answer: (SHOW ANSWER)
Non-final actions are actions that do not terminate the message filter evaluation, such 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.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 3-4.
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_01000.html

NEW QUESTION: 90

An engineer must configure the message source when integrating Cisco Secure Email Threat Defense with Microsoft 365. The integration must allow visibility but not remediation. Drag and drop the actions from the left into sequence on the right to meet the requirement.



Answer:



Explanation:

Step 1: Select Microsoft O365 as the message source.

Step 2: Set the Microsoft 365 Authentication to Read (visibility only, no remediation).

Step 3: Log in with a Microsoft 365 Global Admin account.

Step 4: Accept the permissions requested for the Secure Email Threat Defense app.

NEW QUESTION: 91
Which two features are applied to either incoming or outgoing mail policies? (Choose two.)
A. Indication of Compromise
B. application filtering
C. outbreak filters
D. sender reputation filtering
E. antivirus
Answer: (SHOW ANSWER)
Outbreak filters and antivirus are two features that can be applied to either incoming or outgoing mail policies on Cisco ESA. Outbreak filters allow Cisco ESA to detect and block messages that contain new or emerging email threats, such as viruses, worms, phishing, or spam, by using real-time updates from Talos intelligence.
Antivirus allows Cisco ESA to scan messages for known viruses and malware using one or two antivirus engines (Sophos and McAfee).
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-16 and page 7-2.
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_01001.html

NEW QUESTION: 92
When the Cisco ESA is configured to perform antivirus scanning, what is the default timeout value?
A. 30 seconds
B. 90 seconds
C. 60 seconds
D. 120 seconds
Answer: (SHOW ANSWER)
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.
References: User Guide for Async OS 15.0 for Cisco Secure Email Gateway , page 7-3.
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_01011.html

NEW QUESTION: 93
When DKIM signing is configured, which DNS record must be updated to load the DKIM public signing key?
A. AAAA record
B. PTR record
C. TXT record
D. MX record

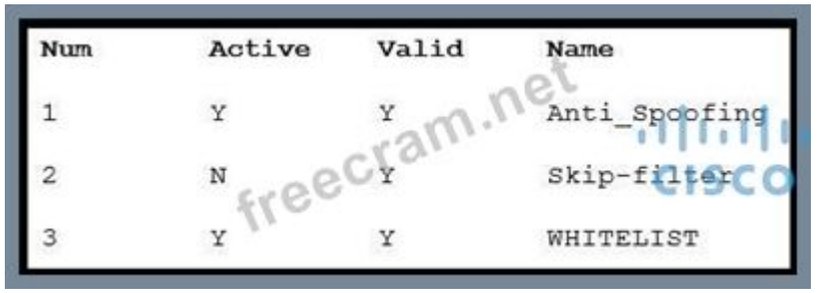
Answer: (SHOW ANSWER)

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.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 11-3.

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

NEW QUESTION: 94



Num	Active	Valid	Name
1	Y	Y	Anti_Spoofing
2	N	Y	Skip-filter
3	Y	Y	WHITELIST

Refer to the exhibit. What is the correct order of c ommands to set filter 2 to active?

A. filters- > edit- > 2- > Active

B. filters- > modify- > All- > Active

C. filters- > detail- > 2- > 1

D. filters- > set- > 2- > 1

Answer: (SHOW ANSWER)

The correct order of commands to set filter 2 to active on the CLI of Cisco ESA is:

* filters, which enters the message filter mode.
* set, which sets the status of one or more message filters.
* 2, which specifies the message filter number.
* 1, which sets the status of message filter 2 to active.

The other options are not valid orders of commands to set filter 2 to active on the CLI of Cisco ESA, because they use incorrect commands or parameters.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page A-6 and page A-7.

NEW QUESTION: 95

Which two actions are configured on the Cisco ESA to query LDAP servers? (Choose two.)

A. accept

B. relay

C. delay

D. route

E. reject

Answer: (SHOW ANSWER)

If you store user information within LDAP directories in your network infrastructure you can configure the appliance to query your LDAP servers to accept, route, and authenticate messa ges. 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_011010.html

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_011010.html