GETCERTKEY

GETCERTKEY
100% guarantee you pass IT cert exam!

http://www.getcertkey.com

No help, Full refund!

Exam : **300-720**

Title : Securing Email with Cisco Email Security Appliance

Vendor : Cisco

Version : DEMO

NO.1 Spammers routinely try to send emails with the recipient field filled with a list of all possible combinations of letters and numbers. These combinations, appended with a company domain name are malicious attempts at learning all possible valid email addresses. Which action must be taken on a Cisco Secure Email Gateway to prevent this from occurring?

A. Select the SMTP Authentication Query checkbox

B. Perform LDAP acceptance validation.

C. Quarantine external authentication queries.

D. Enable end user safelist features

Answer: B

Explanation:

LDAP acceptance validation is a feature that allows the Cisco Secure Email Gateway to check if the recipient address of an incoming message exists in an LDAP directory before accepti ng it. This feature can help prevent spammers from sending emails with invalid recipient addresses and reduce the load on the applia nce

2 . References = User Guide for AsyncOS 12.0 for Cisco Email Security A ppliances - GD (General Deployment) - Configuring LDAP Queries [Cisco Secure Email Gateway] - Cisco

NO.2 A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy.

What is the reason of this?

A. The Tram* header is checked against all policies in a top-down fashion.

B. The message header with the highest priority is checked ag ainst each policy in a top-down fashion.

C. The message header with the highest priority is checked against the Default policy in a top-down fashion.

D. The To " header is checked against all policies in a top-down fashion.

Answer: B

NO.3 Which Cisco Secure Email Threat Defense visibility and remediation mode is only available when using Cisco Secure Email Gateway as the message source?

A. Basic Authentication

B. No Authentication

C. Microsoft 365 Authentication

D. Cisco Security Cloud Sign On

Answer: B

NO.4 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.

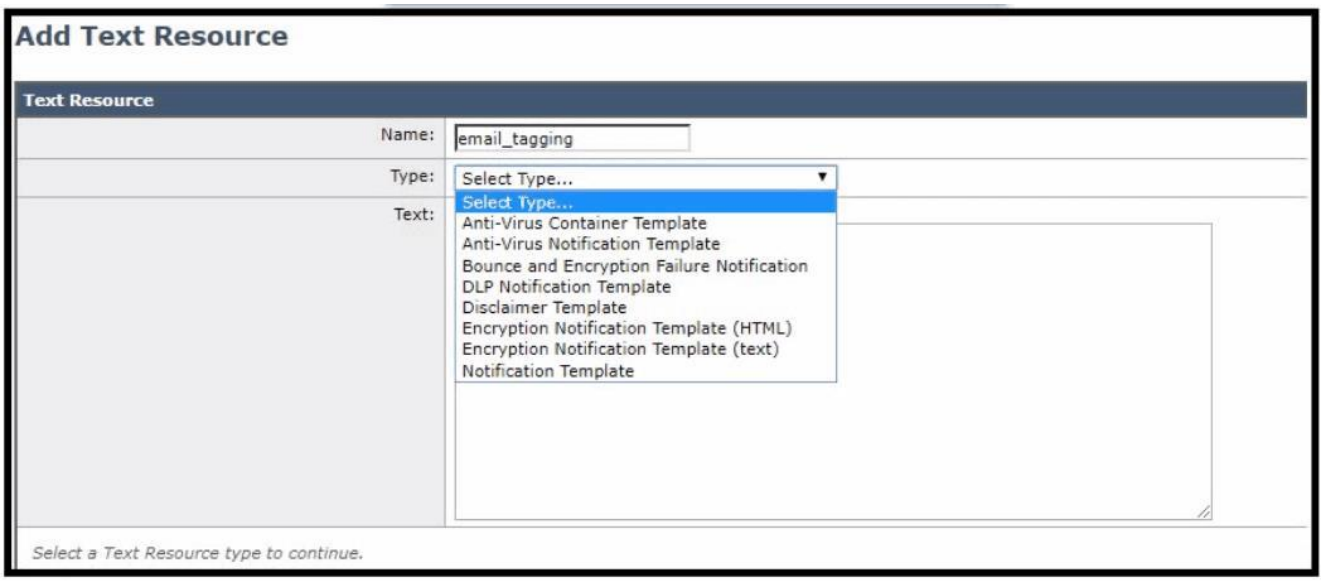
Answer: D

Explanation:

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

NO.5 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: B

Explanation:
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].

NO.6 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: A C
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.

NO.7 Which SMTP extension does Cisco ESA support for email security?
A. ETRN
B. UTF8SMTP
C. PIPELINING
D. STARTTLS
Answer: D
Explanation:
STARTTLS is an SMTP extension that allows email servers to negotiate a secure connection using TLS or SSL encryption. Cisco ESA supports STARTTLS for both inbound and outbound email delivery.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 5-2.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011000.html

NO.8 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: C
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

NO.9

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: D
Explanation:
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.

NO.10 When the spam quarantine is configured on the Cisco Secure Email Gateway, which type of query is used to validate non administrative user access to the end-user quarantine via LDAP?
A. spam quarantine end-user authentication
B. spam quarantine alias consolidation

C. spam quarantine external authorization

D. local mailbox (IMAP/POP) authentication

Answer: A

Explanation:

spam quarantine end-user authentication query is used to validate non administrative user access to the end- user quarantine via LDAP 1 . This query is configured in the System Admini stration > LDAP > LDAP Server Profile page and can be tested using the smtproutes command in the CLI 1 . The other queries are not related to this task. The spam quarantine alias consolidation query is used to consolidate multiple email addresses for a user into one login 2 . The spam quarantin e external authorization query is used to authorize users to access an external spam quarantine on a separate Cisco Secure Email and Web Manager 3 . The local mailbox (IMAP/POP) authentication is an alternative method to authenticate users without using LDAP 2 .

NO.11 A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy.

What is the reason of this?

A. The Tram* header is checked against all policies in a top-down fashion.

B. The message header with the highest priority is checked ag ainst each policy in a top-down fashion.

C. The To " header is checked against all policies in a top-down fashion.

D. The message header with the highest priority is checked against the Default policy in a top-down fashion.

Answer: B

Explanation:

The envelope sender and the envelope recipeint have a higher priority over the sender header when you match a message to a mail policy. If you configure a mail policy to match a specific user, the messages are automatically classified into the mail policy based on the envelo pe sender and the envelope recipient.

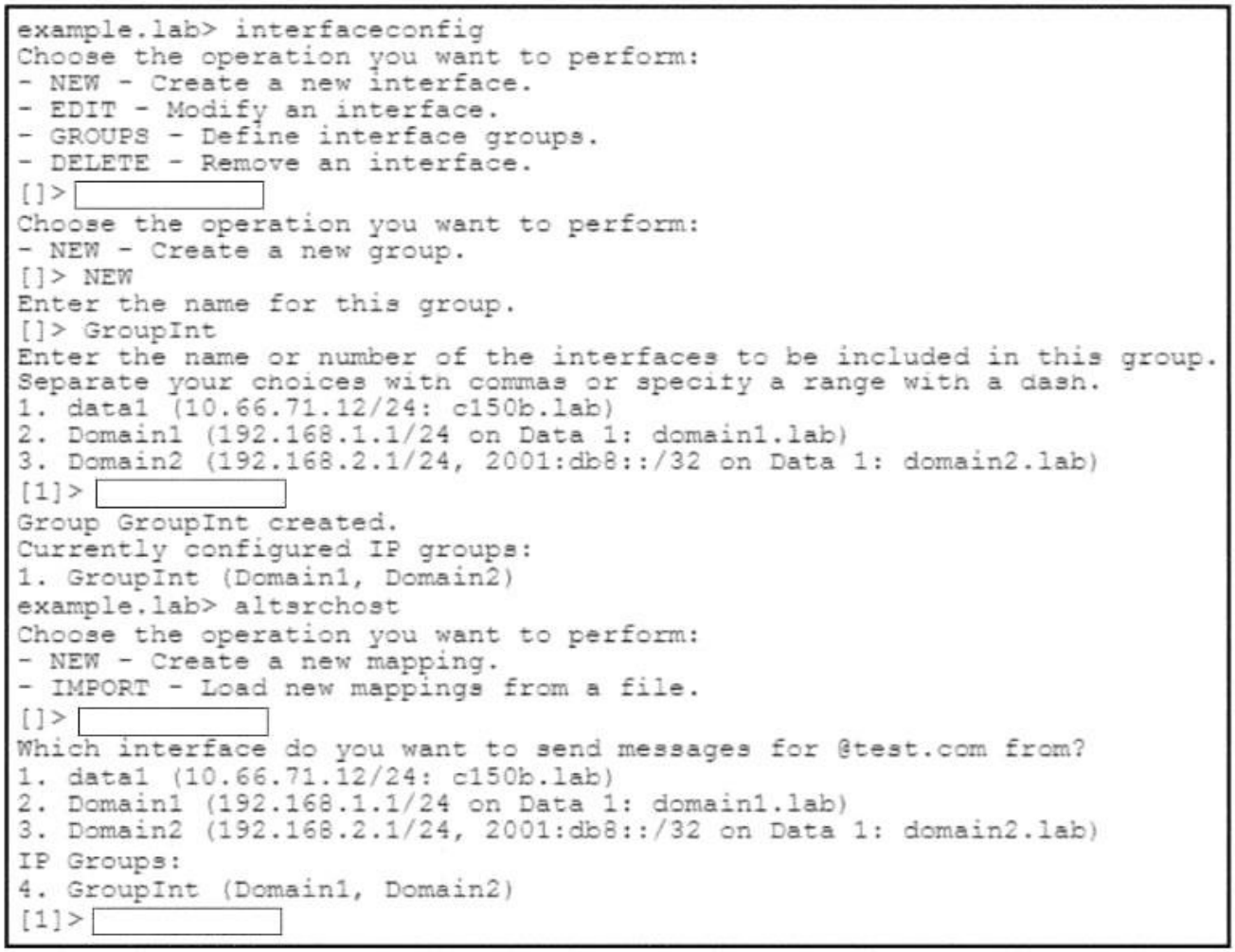
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01001.html

NO.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

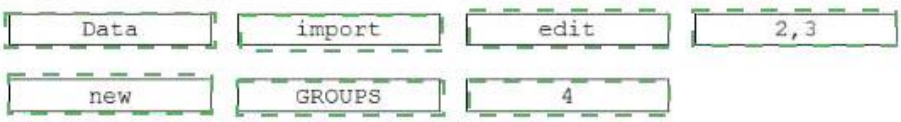
Drag and drop the code snippets from the right onto the boxes to configure the virtual gateway. Not all options are used.



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
```

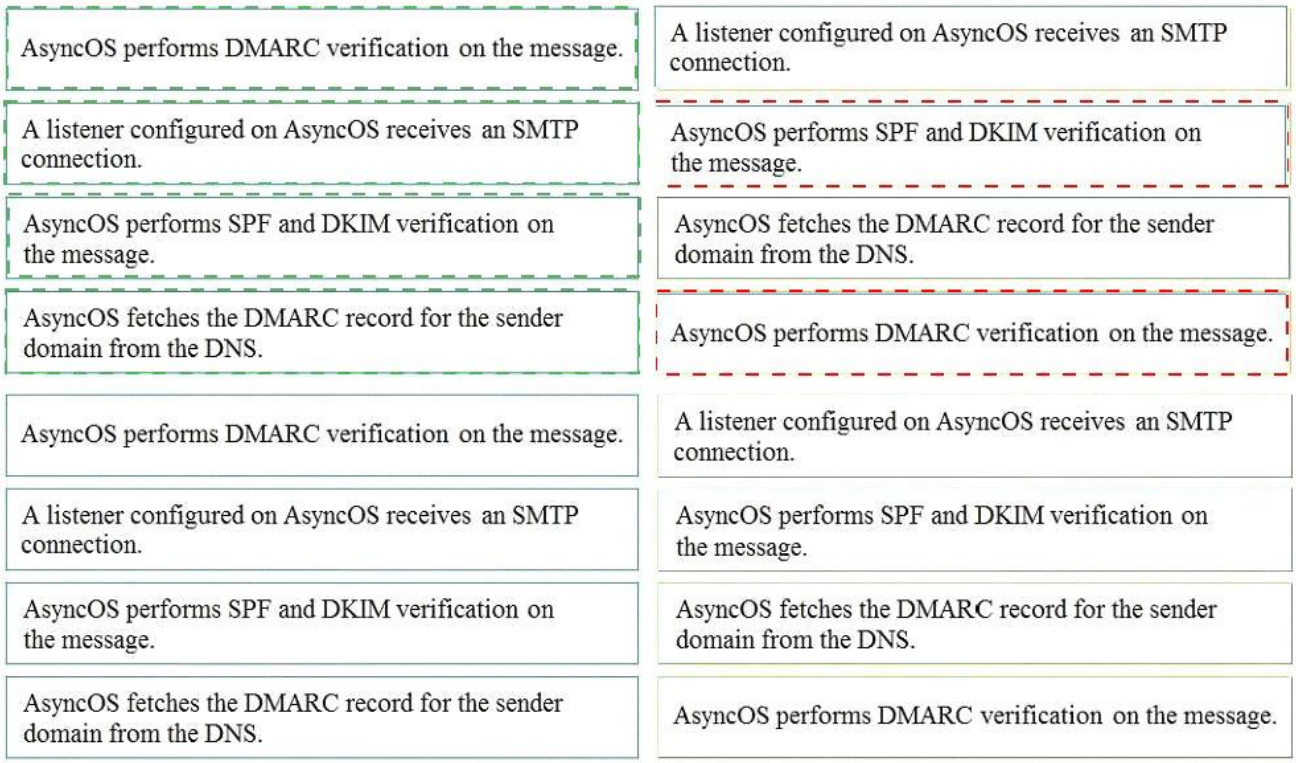


```
example.lab> interfaceconfig
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> GROUPS
Choose the operation you want to perform:
- NEW - Create a new group.
[]> NEW
Enter the 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 specity 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
```

NO.13 Drag and drop the AsyncOS methods for performing DMARC verification from the left into the correct order on the right.

AsyncOS performs DMARC verification on the message.	step 1
A listener configured on AsyncOS receives an SMTP connection.	step 2
AsyncOS performs SPF and DKIM verification on the message.	step 3
AsyncOS fetches the DMARC record for the sender domain from the DNS.	step 4

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_010101.html

NO.14 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: A E

Explanation:

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)

NO.15 Which action do Outbreak Filters take to stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites?

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 harm ful 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 phishi ng scams and malware distribution sites, that may not be detected by other filters. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Outbreak Filters]

NO.16 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: A E
Explanation:
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

NO.17

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]>

Proxy: Not Configured

Profile Name Key Service Proxied Provision Status
------------ ----------- ------- ----------------
CRES HIGH      Hosted     Service  No Provisioned
```

Refer to the exhibit. A security engineer must configure a Cisco Secure Email Gateway to ensure that encryption is enabled and the configured profile is provisioned. Which command must be used?

A. setup

B. check encryption

C. provision

D. profiles

Answer: C

NO.18 Which predefined DLP category must be used by a network administrator to ensure that a company employee cannot send credit card information outside the company?

A. Company Confidential

B. Regulatory Compliance

C. Intellectual Property Protection

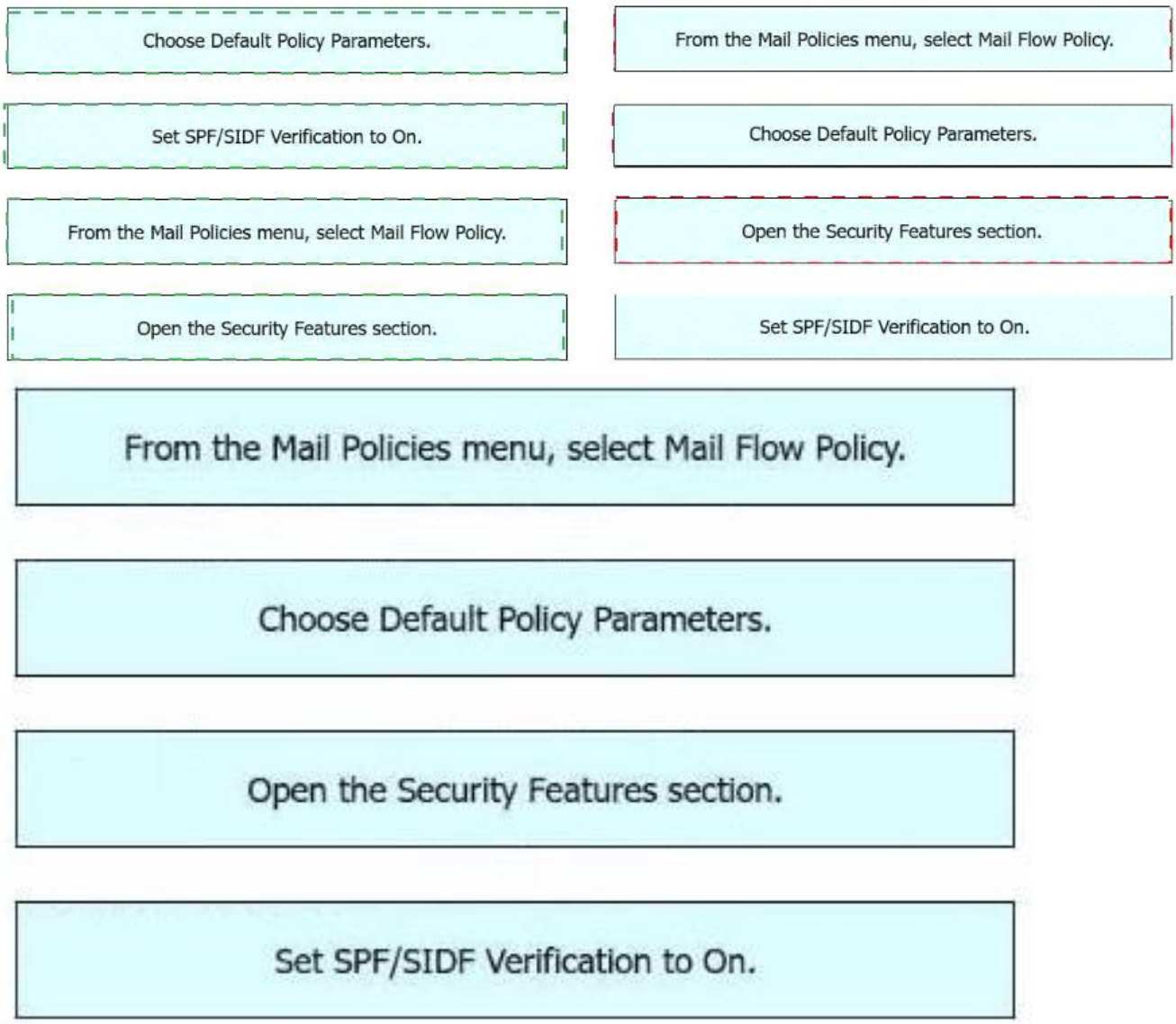
D. Acceptable Use

Answer: B

NO.19 Drag and drop the actions from the left into sequence on the right to validate the authenticity of email on a Cisco Secure Email Gateway by using DNS records.

Choose Default Policy Parameters.	step 1
Set SPF/SIDF Verification to On.	step 2
From the Mail Policies menu, select Mail Flow Policy.	step 3
Open the Security Features section.	step 4

Answer:


Choose Default Policy Parameters.
From the Mail Policies menu, select Mail Flow Policy.
Set SPF/SIDF Verification to On.
Choose Default Policy Parameters.
From the Mail Policies menu, select Mail Flow Policy.
Open the Security Features section.
Open the Security Features section.
Set SPF/SIDF Verification to On.
From the Mail Policies menu, select Mail Flow Policy.
Choose Default Policy Parameters.
Open the Security Features section.
Set SPF/SIDF Verification to On.