300-720$^{Q\&As}$

Securing Email with Cisco Email Security Appliance (SESA)

Pass Cisco 300-720 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-720.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?

A. Set up the interface group with the flag.

B. Issue the altsrchost command.

C. Map the envelope sender address to the host.

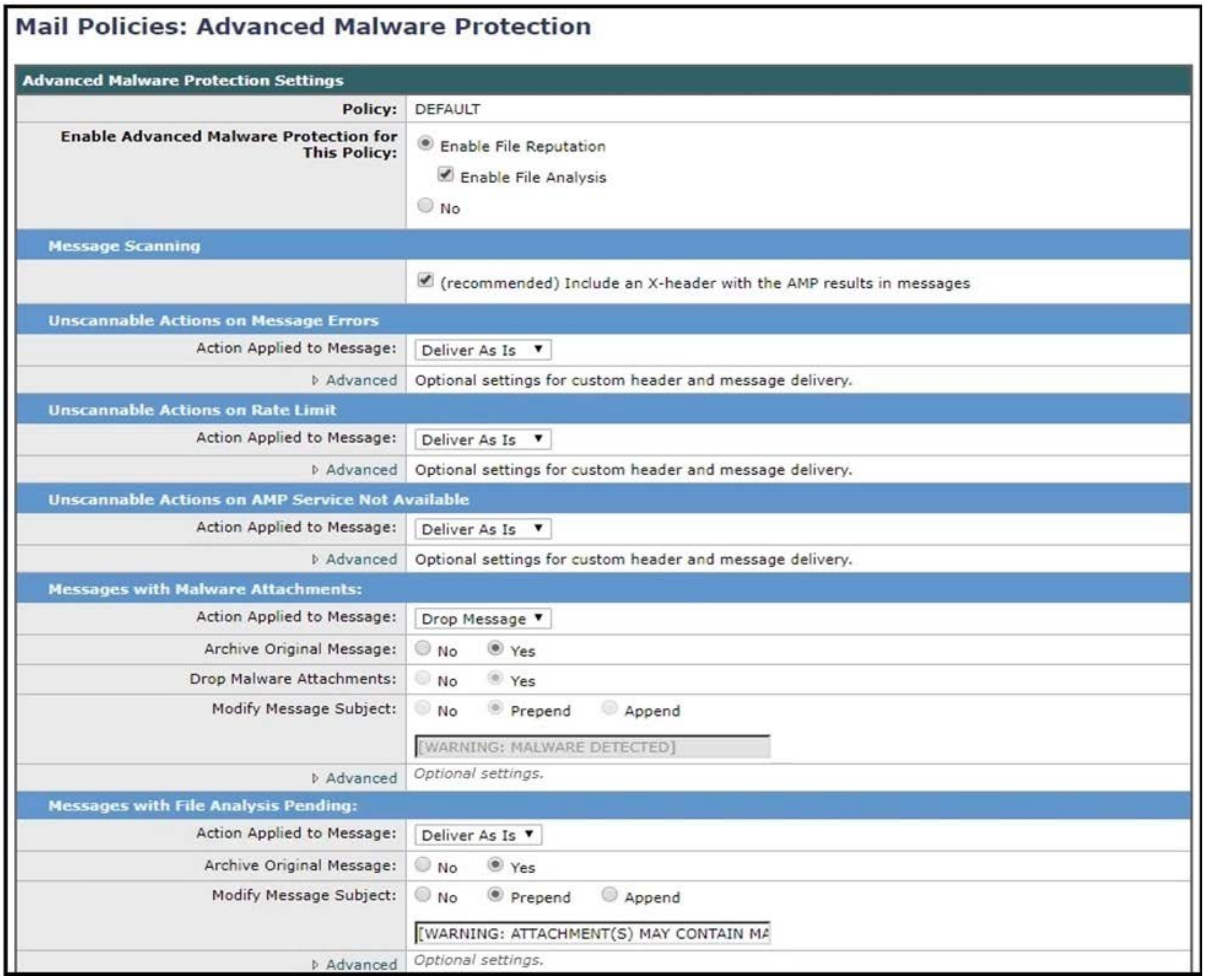
D. Apply a filter on the message.

Correct Answer: B

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#con_1133810

QUESTION 2

Refer to the exhibit.



Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	● Enable File Reputation ☑ Enable File Analysis ○ No
Message Scanning	
	☑ (recommended) Include an X-header with the AMP results in messages
Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is ▼
▹ Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is ▼
▹ Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is ▼
▹ Advanced	Optional settings for custom header and message delivery.
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
Archive Original Message:	○ No ● Yes
Drop Malware Attachments:	○ No ● Yes
Modify Message Subject:	○ No ● Prepend ○ Append [WARNING: MALWARE DETECTED]
▹ Advanced	*Optional settings.*
Messages with File Analysis Pending:	
Action Applied to Message:	Deliver As Is ▼
Archive Original Message:	○ No ● Yes
Modify Message Subject:	○ No ● Prepend ○ Append [WARNING: ATTACHMENT(S) MAY CONTAIN MA
▹ Advanced	*Optional settings.*

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.

Correct Answer: C

QUESTION 3

What is a benefit of deploying Cisco Secure Email and Web Manager?

A. centralized management of software updates for Cisco Secure Email Gateway

B. centralized management of logs for Cisco Secure Email Gateway

C. centralized management of quarantined email

D. centralized management of botnet directories

Correct Answer: C

One of the benefits of deploying Cisco Secure Email and Web Manager is that it provides centralized management of quarantined email for multiple Cisco Secure Email Gateway appliances. The administrator can use the Cisco Secure Email and Web Manager to view, search, release, delete, or forward quarantined messages from a single web interface. References: [Cisco Secure Email and Web Manager User Guide - Configuring Centralized Spam Quarantine]

QUESTION 4

A Cisco ESA administrator must provide outbound email authenticity and configures a DKIM signing profile to handle this task. What is the next step to allow this organization to use DKIM for their outbound email?

A. Configure the Trusted Sender Group message authenticity policy.

B. Export the DNS TXT record to provide to the DNS registrar.

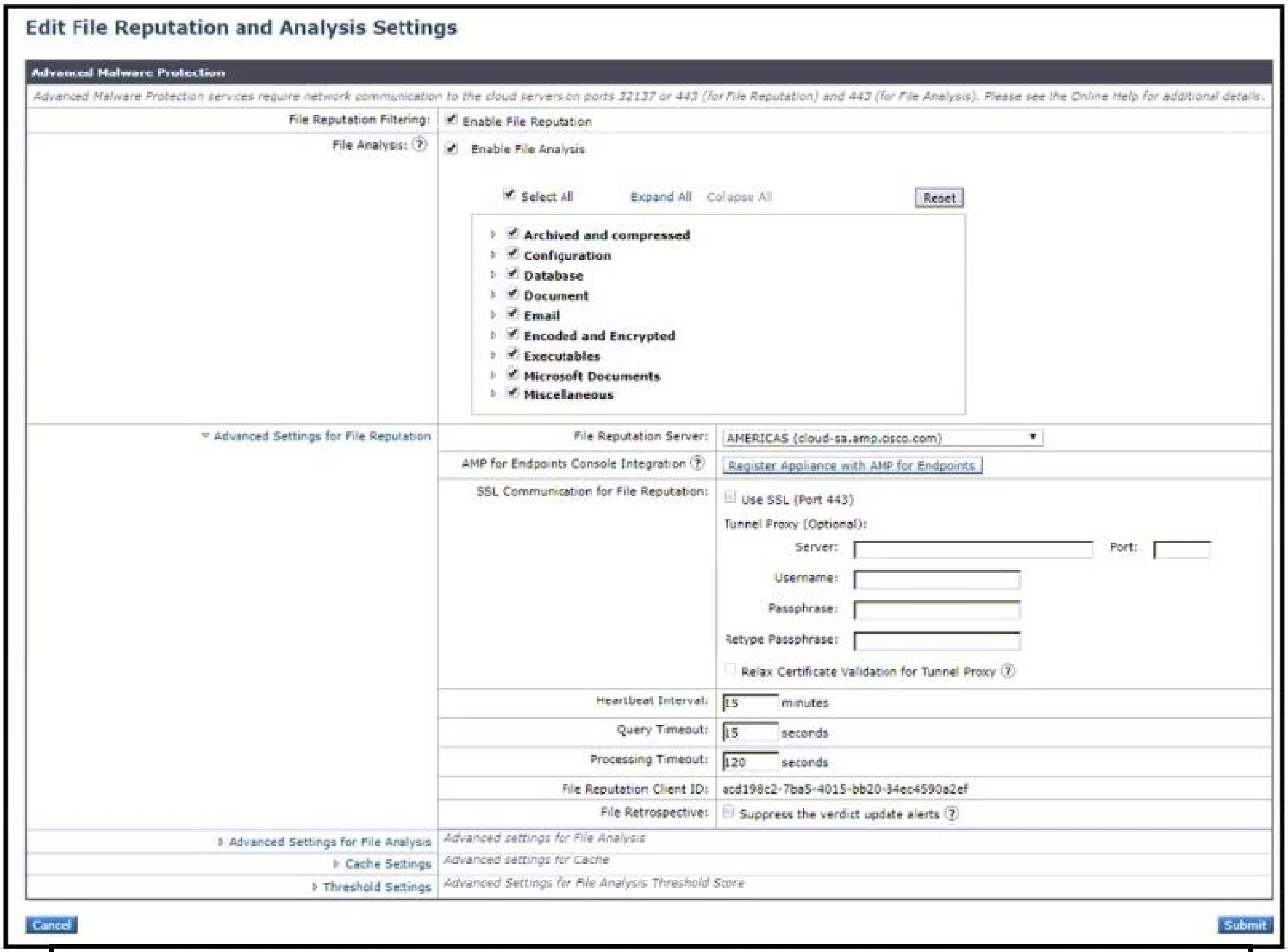
C. Import the DNS record of the service provider into the Cisco ESA.

D. Enable the DKIM service checker.

Correct Answer: C

QUESTION 5

Refer to the exhibit.



Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering: ☑ Enable File Reputation

File Analysis: ☑ Enable File Analysis

☑ Select All Expand All Collapse All Reset

- ☑ Archived and compressed
- ☑ Configuration
- ☑ Database
- ☑ Document
- ☑ Email
- ☑ Encoded and Encrypted
- ☑ Executables
- ☑ Microsoft Documents
- ☑ Miscellaneous

Advanced Settings for File Reputation

File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com)

AMP for Endpoints Console Integration: Register Appliance with AMP for Endpoints

SSL Communication for File Reputation: ☐ Use SSL (Port 443)

Tunnel Proxy (Optional):

Server: Port:

Username:

Passphrase:

Retype Passphrase:

☐ Relax Certificate Validation for Tunnel Proxy

Heartbeat Interval: 15 minutes

Query Timeout: 15 seconds

Processing Timeout: 120 seconds

File Reputation Client ID: acd198c2-7ba5-4015-bb20-34ec4590a2ef

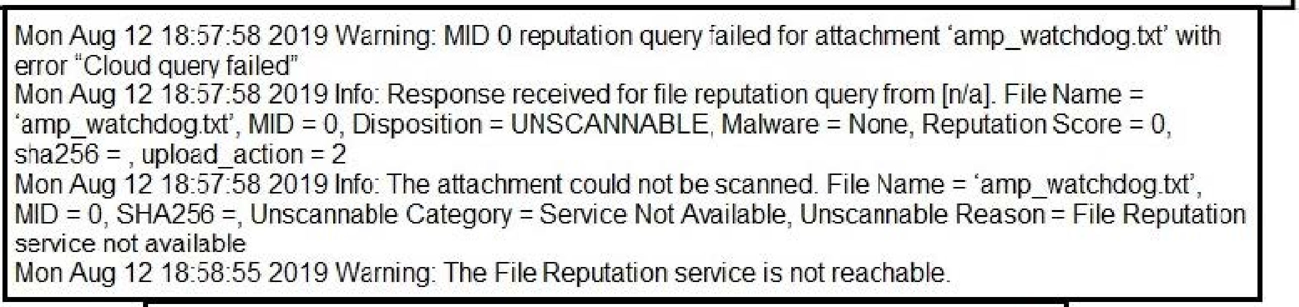
File Retrospective: ☐ Suppress the verdict update alerts

Advanced Settings for File Analysis — *Advanced settings for File Analysis*

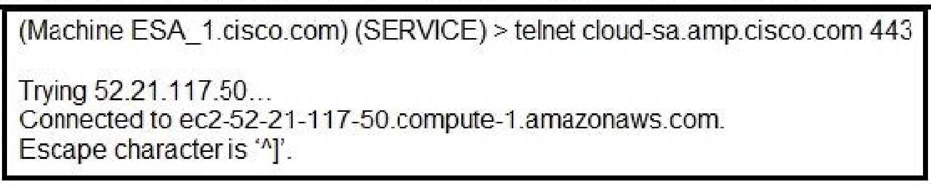
Cache Settings — *Advanced settings for Cache*

Threshold Settings — *Advanced Settings for File Analysis Threshold Score*

Cancel
Submit



```
Mon Aug 12 18:57:58 2019 Warning: MID 0 reputation query failed for attachment 'amp_watchdog.txt' with
error "Cloud query failed"
Mon Aug 12 18:57:58 2019 Info: Response received for file reputation query from [n/a]. File Name =
'amp_watchdog.txt', MID = 0, Disposition = UNSCANNABLE, Malware = None, Reputation Score = 0,
sha256 = , upload_action = 2
Mon Aug 12 18:57:58 2019 Info: The attachment could not be scanned. File Name = 'amp_watchdog.txt',
MID = 0, SHA256 =, Unscannable Category = Service Not Available, Unscannable Reason = File Reputation
service not available
Mon Aug 12 18:58:55 2019 Warning: The File Reputation service is not reachable.
```



```
(Machine ESA_1.cisco.com) (SERVICE) > telnet cloud-sa.amp.cisco.com 443

Trying 52.21.117.50...
Connected to ec2-52-21-117-50.compute-1.amazonaws.com.
Escape character is '^]'.
```

An administrator has configured File Reputation and File Analysis on the Cisco ESA; however, is does not function as expected. What must be configured on the Cisco ESA for this to function?

A. Upload the Root CA certificate for the File Reputation cloud to the Cisco ESA.

B. Open port 443 on the firewall for the Cisco ESA to connect to the File Reputation cloud.

C. Restart the File Reputation service to force the scanning engine to connect to the File Reputation cloud.

D. Configure the Cisco ESA to use SSL for the connection to the File Reputation server.

Correct Answer: A

QUESTION 6

Which antispam feature is utilized to give end users control to allow emails that are spam to be delivered to their inbox, overriding any spam verdict and action on the Cisco ESA?

A. end user allow list

B. end user spam quarantine access

C. end user passthrough list

D. end user safelist

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_011111.pdf

QUESTION 7

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. SPF Verification

B. Duplicate Boundaries Verification

C. Forged Email Detection

D. Subject Header

Correct Answer: C

QUESTION 8

What is a benefit of deploying Cisco SMA?

A. centralized management of logs for Cisco ESA appliances

B. centralized management of botnet directories

C. centralized management of software updates for Cisco ESA appliances

D. centralized management of quarantined email

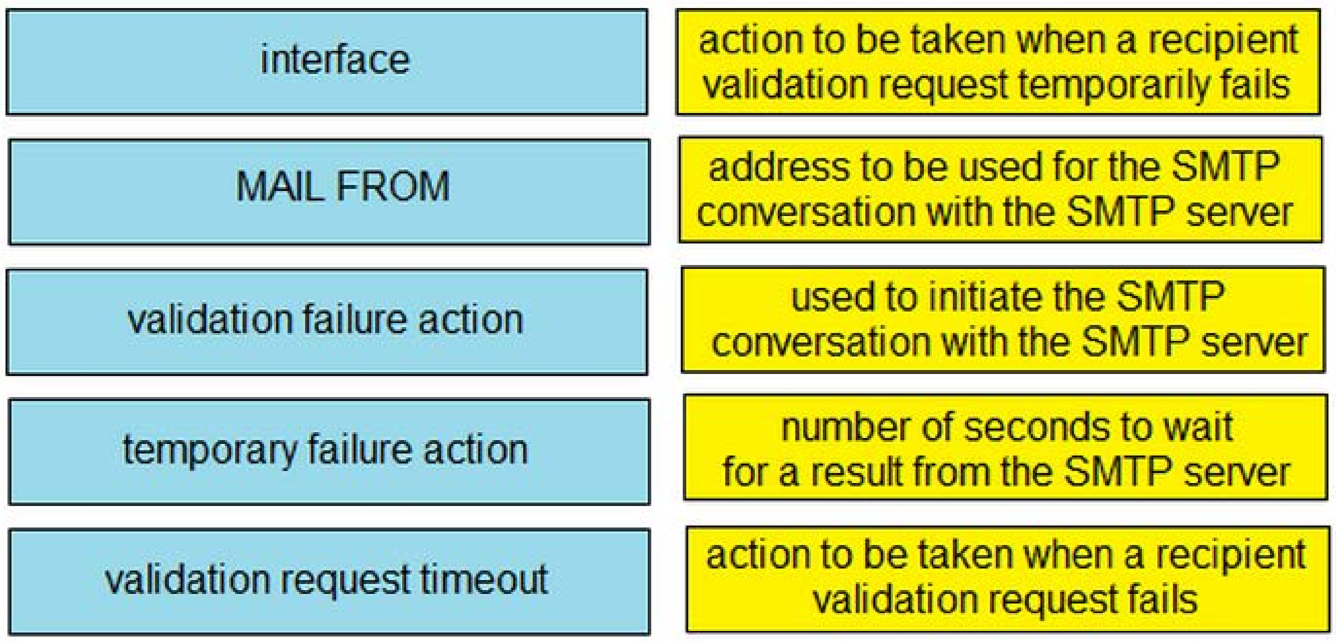
Correct Answer: C

QUESTION 9

DRAG DROP

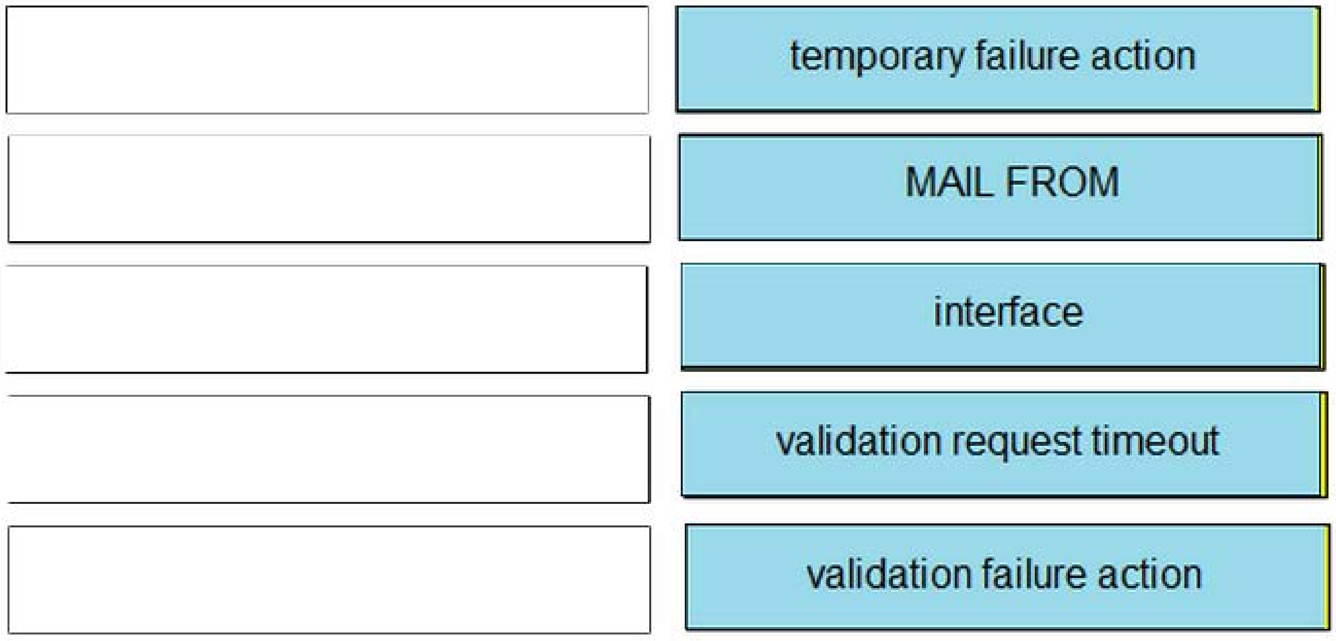
Drag and drop the SMTP Call-Ahead Server Profile Settings from the left onto the descriptions on the right.

Select and Place:



interface	action to be taken when a recipient validation request temporarily fails
MAIL FROM	address to be used for the SMTP conversation with the SMTP server
validation failure action	used to initiate the SMTP conversation with the SMTP server
temporary failure action	number of seconds to wait for a result from the SMTP server
validation request timeout	action to be taken when a recipient validation request fails

Correct Answer:



	temporary failure action
	MAIL FROM
	interface
	validation request timeout
	validation failure action

QUESTION 10

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 a Cisco ESA and determines that the message was dropped by the antivirus engine. What is the reason for this behavior?

A. End-user safelists apply to antispam engines only.

B. The sender didn\\'t mark the message as urgent.

C. Administrative access is required to create a safelist.

D. The sender is included in an ISP blocklist.

Correct Answer: A

QUESTION 11

Users have been complaining of a higher volume of emails containing profanity. The network administrator will need to leverage dictionaries and create specific conditions to reduce the number of inappropriate emails.

Which two filters should be configured to address this? (Choose two.)

A. message

B. spam

C. VOF

D. sender group

E. content

Correct Answer: BE

QUESTION 12

A company security policy requires that the finance department have an easy way to apply encryption to their outbound messages that contain sensitive data. Users must be able to flag the messages that require encryption versus a Cisco ESA scanning all messages and automatically encrypting via detection. Which action enables this capability?

A. Create an outgoing content filter with no conditions and with the Encrypt and Deliver Now action configured with [SECURE] in the Subject setting.

B. Create a DLP policy manager message action with encryption enabled and apply it to active DLP policies for outgoing mail.

C. Create an encryption profile with [SECURE] in the Subject setting and enable encryption on the mail flow policy.

D. Create an encryption profile and an outgoing content filter that includes \[SECURE\] within the Subject Header: Contains condition along with the Encrypt and Deliver Now action.

Correct Answer: D

QUESTION 13

A Cisco ESA is configured such that emails with a reputation score above -6 are logged and those with a score below -6 are logged, encrypted, and then delivered. An email body contains a shortened URL that exceeds the nested shortened URLs limit. Which action is taken against the email?

A. It is encrypted but not logged.

B. It is logged but not encrypted.

C. It is logged and dropped.

D. It is logged and encrypted.

Correct Answer: A