Cisco.300-720.v2022-04-15.q59

Exam Code:	300-720
Exam Name:	Securing Email with Cisco Email Security Appliance
Certification Provider:	Cisco
Free Question Number:	59
Version:	v2022-04-15
# of views:	1593
# of Questions views:	590
https://www.exam-tests.com/300-720-exam/Cisco.300-720.v2022-04-15.q59.html	

NEW QUESTION: 1
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: C (LEAVE A REPLY)
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: 2
Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?
A. Map the envelope sender address to the host.
B. Set up the interface group with the flag.
C. Apply a filter on the message.
D. Issue the altsrchost command.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
Spreadsheets containing credit card numbers are being allowed to bypass the Cisco ESA.
Which outgoing mail policy feature should be configured to catch this content before it leaves the network?
A. outbreak filtering
B. file reputation filtering
C. file analysis
D. data loss prevention
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Which feature must be configured before an administrator can use the outbreak filter for nonviral threats?
A. antivirus
B. data loss prevention
C. quarantine threat level
D. antispam
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
When virtual gateways are configured, which two distinct attributes are allocated to each virtual gateway address? (Choose two.)
A. external spam quarantine
B. DNS server address
C. IP address
D. DHCP server address
E. domain
Answer: (SHOW ANSWER)

NEW QUESTION: 6
When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)
A. redirect
B. return
C. drop
D. delay
E. abandon
Answer: (SHOW ANSWER)
Explanation/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_01110.html

NEW QUESTION: 7
Which two actions are configured on the Cisco ESA to query LDAP servers? (Choose two.)
A. relay
B. accept
C. reject
D. delay
E. route
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 8
Which action on the Cisco ESA provides direct access to view the safelist/blocklist?

A. Show the SLBL cache on the CLI.
B. Monitor Incoming/Outgoing Listener.
C. Export the SLBL to a .csv file.
D. Debug the mail flow policy.
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117922-technote- esa-00.html

NEW QUESTION: 9
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: C,E (LEAVE A REPLY)
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: 10
Which two steps are needed to disable local spam quarantine before external quarantine is enabled? (Choose two.)
A. Select Security Services and click Spam Quarantine.
B. Select External Spam Quarantine and click on Configure.
C. Select Monitor and click Spam Quarantine.
D. Check the External Safelist/Blocklist check box.
E. Uncheck the Enable Spam Quarantine check box.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)
A. delay
B. drop
C. redirect
D. abandon
E. return
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 12
When the Spam Quarantine is configured on the Cisco ESA, what validates end-users via LDAP during login to the End-User Quarantine?
A. Enabling the End-User Safelist/Blocklist feature
B. Spam Quarantine External Authentication Query

C. Spam Quarantine End-User Authentication Query
D. Spam Quarantine Alias Consolidation Query
Answer: C (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure- esa-00.html

NEW QUESTION: 13
Email encryption is configured on a Cisco ESA that uses CRES.
Which action is taken on a message when CRES is unavailable?
A. It is encrypted by a Cisco encryption appliance.
B. It is sent in clear text.
C. It is dropped and an error message is sent to the sender.
D. It is requeued.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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. Modify the Routing Tables and add a route for IP address to 192.168.1.10.
B. Add an address list for domain abc.com.
C. Modify Destination Controls entry for the domain abc.com.
D. Modify the SMTP route for the domain and change the IP address to 192.168.1.10.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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. content
B. message
C. spam
D. VOF
E. sender group
Answer: (SHOW ANSWER)

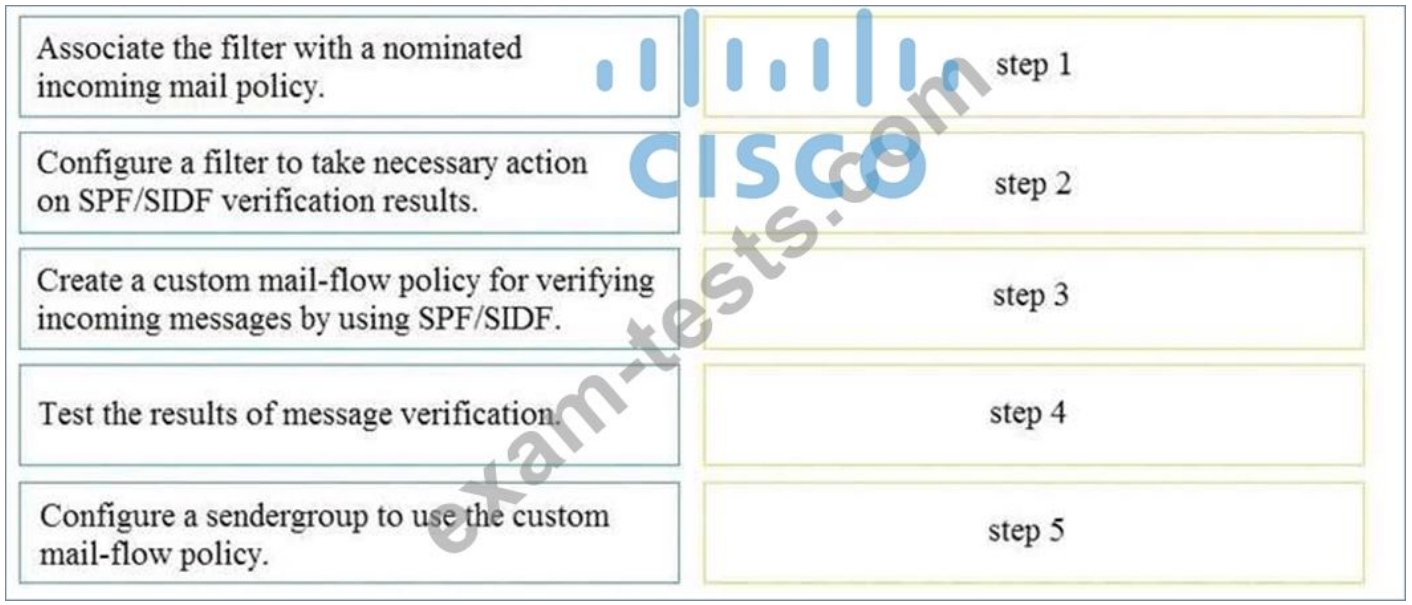
NEW QUESTION: 16
When URL logging is configured on a Cisco ESA, which feature must be enabled first?
A. antivirus
B. antispam

C. virus outbreak filter
D. senderbase reputation filter
Answer: C (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote- esa-00.html (note under enable url filtering)

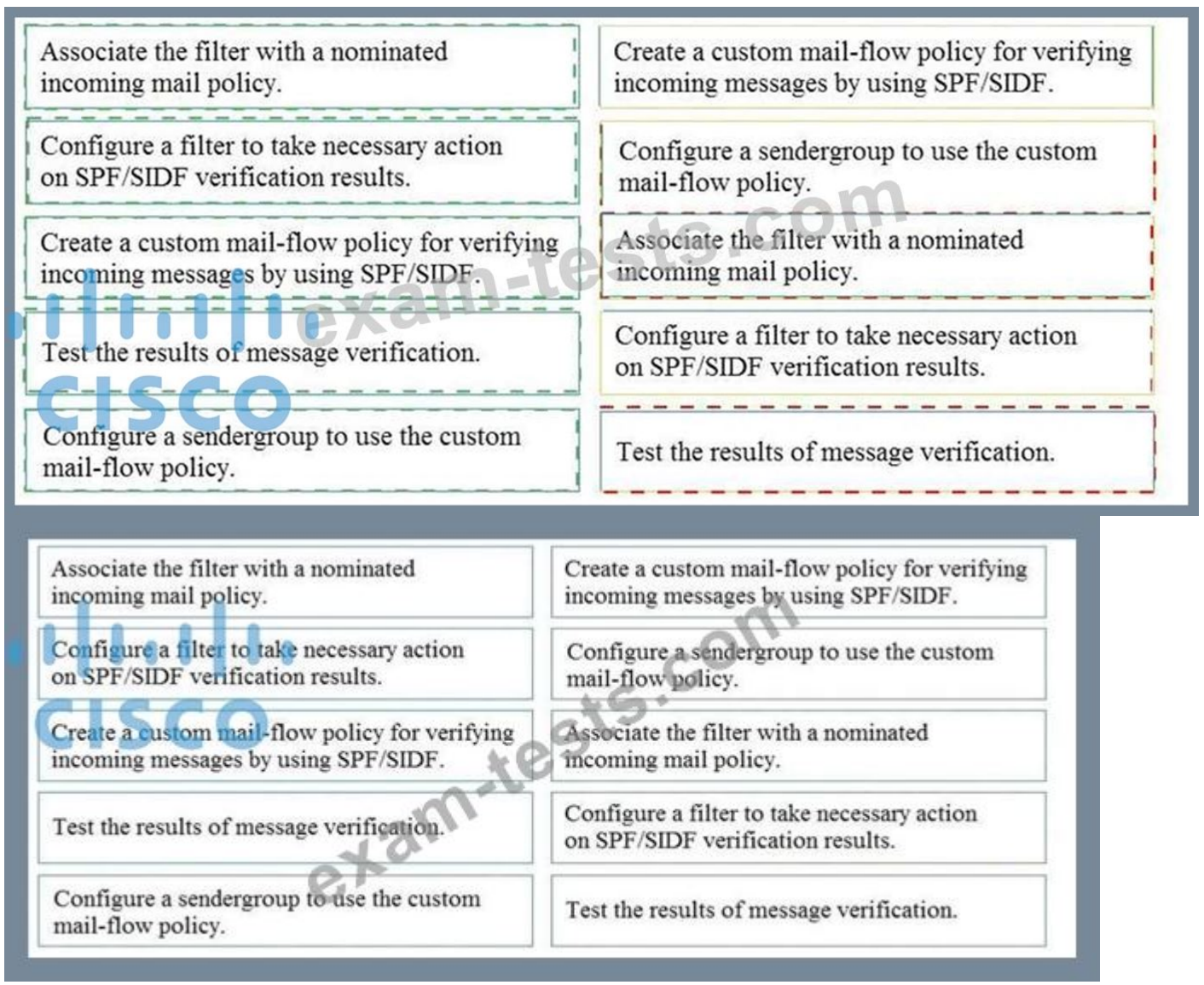
NEW QUESTION: 17
Which global setting is configured under Cisco ESA Scan Behavior?
A. attachment scanning timeout
B. actions for unscannable messages due to attachment type
C. minimum attachment size to scan
D. minimum depth of attachment recursion to scan
Answer: (SHOW ANSWER)

NEW QUESTION: 18
What are two primary components of content filters? (Choose two.)
A. conditions
B. subject
C. content
D. actions
E. policies
Answer: (SHOW ANSWER)
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_01010.pdf

NEW QUESTION: 19
Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.



Answer:



NEW QUESTION: 20

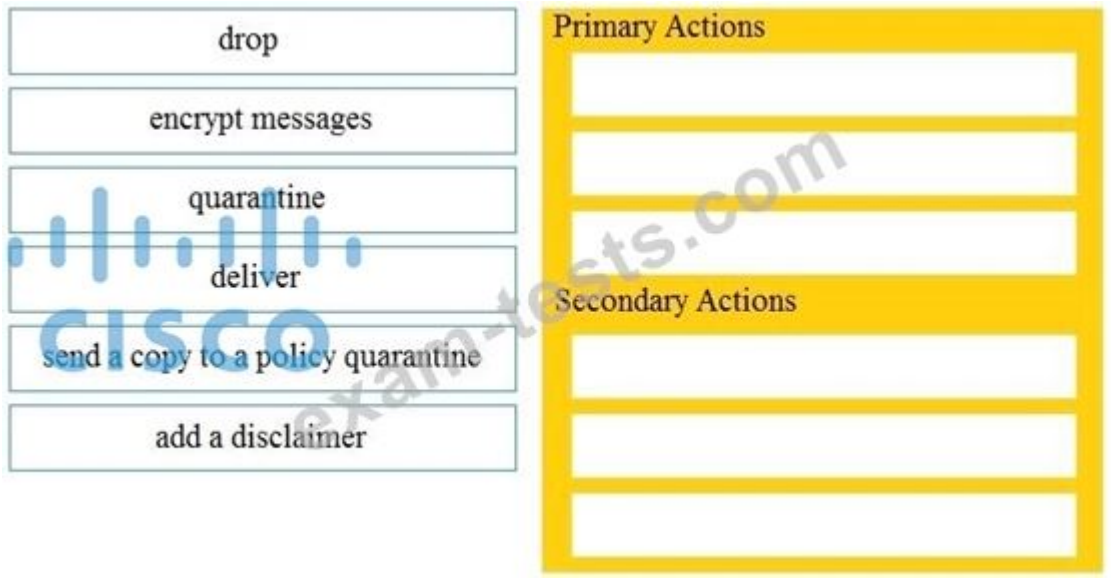
What occurs when configuring separate incoming mail policies?

A. message aggregation

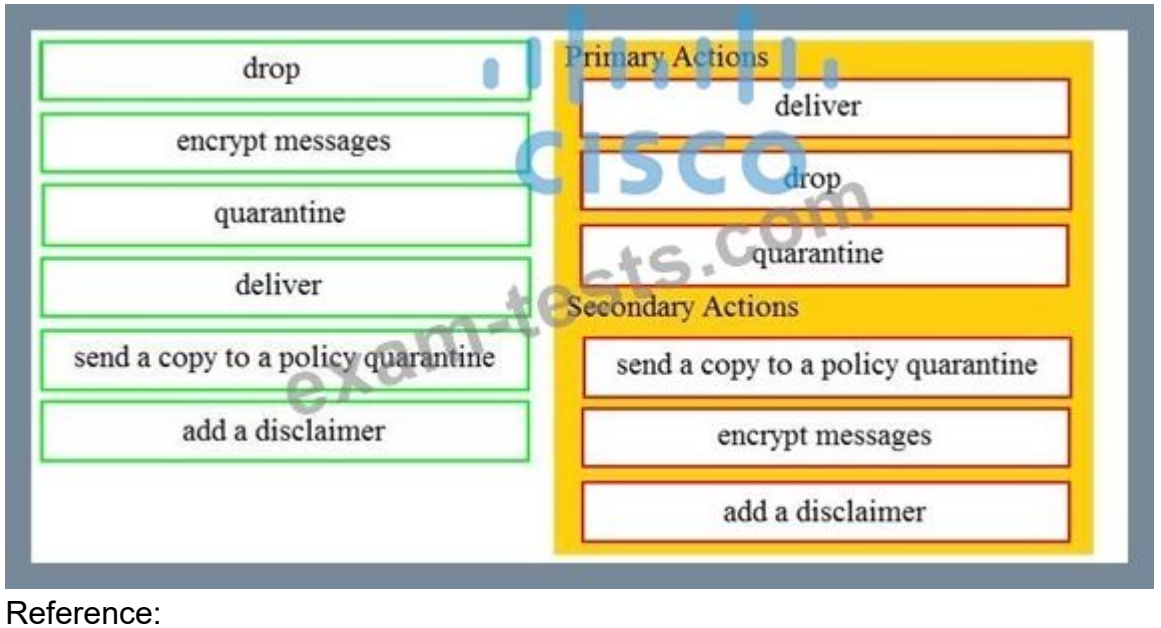
B. message detachment
C. message splintering
D. message exceptions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
Which action is a valid fallback when a client certificate is unavailable during SMTP authentication on Cisco ESA?
A. LDAP Query
B. SMTP TLS
C. SMTP AUTH
D. LDAP BIND
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
Drag and drop the Cisco ESA reactions to a possible DLP from the left onto the correct action types on the right.



Answer:

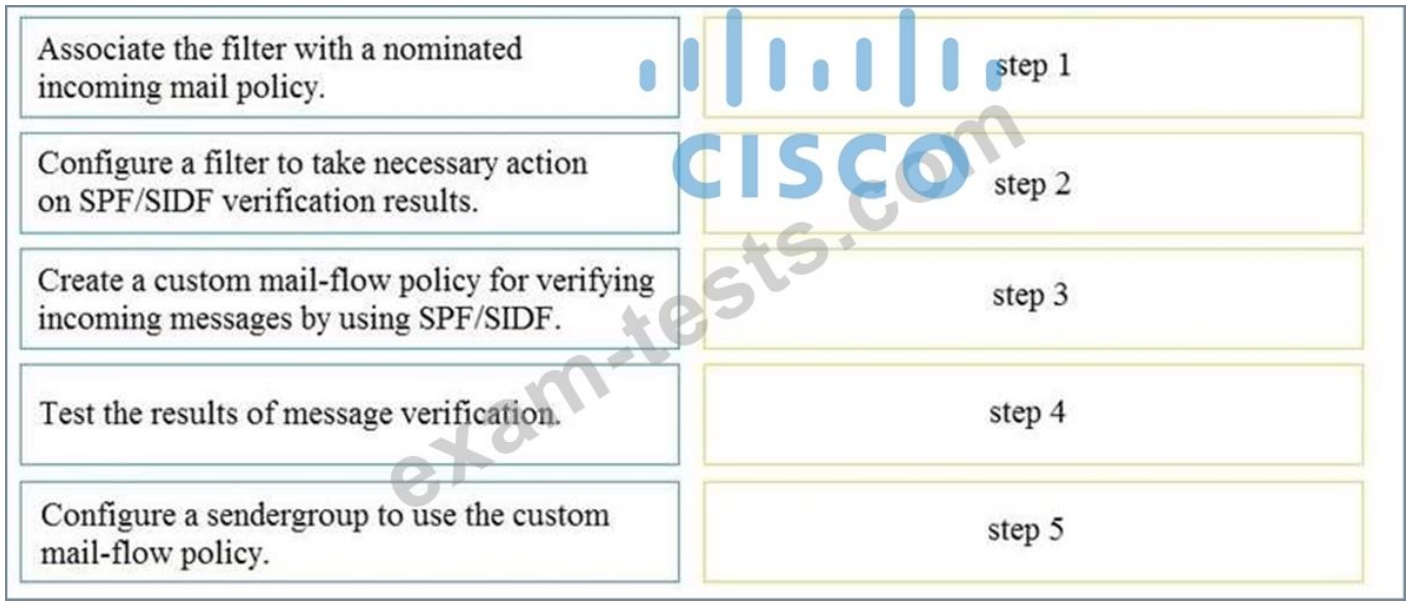


Reference:

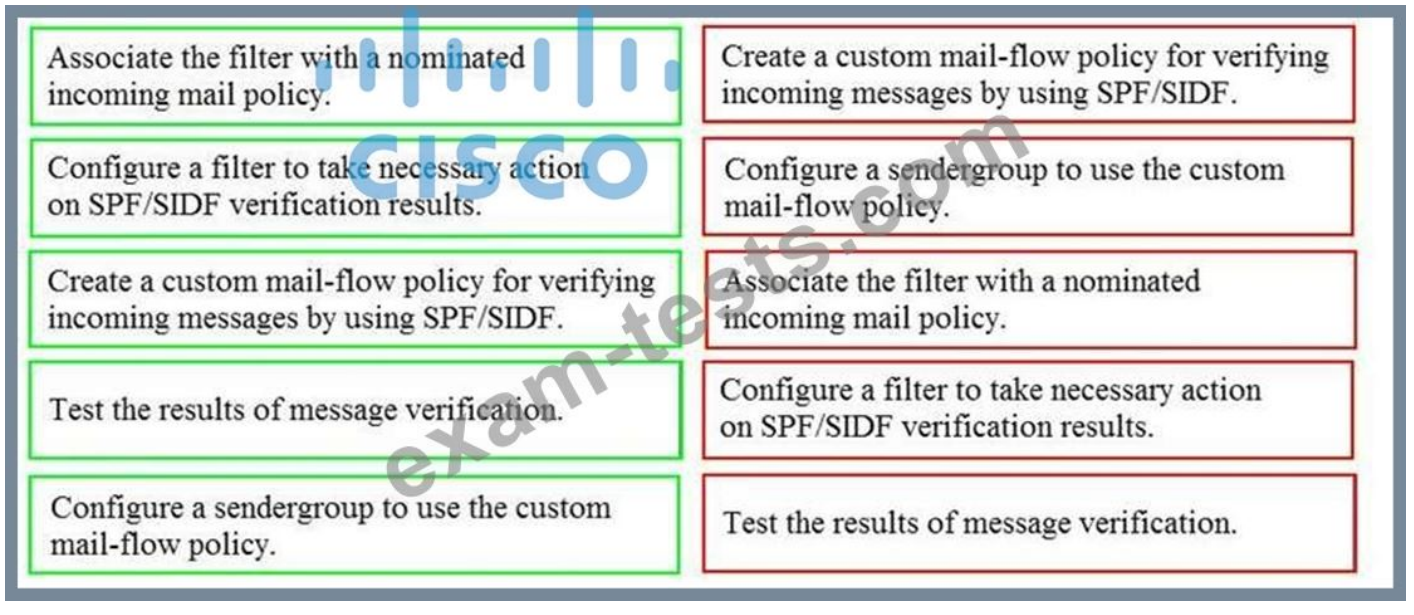
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html (message actions)

NEW QUESTION: 23
An engineer is configuring a Cisco ESA for the first time and needs to ensure that any email traffic coming from the internal SMTP servers is relayed out through the Cisco ESA and is tied to the Outgoing Mail Policies.
Which Mail Flow Policy setting should be modified to accomplish this goal?
A. Exception List
B. Connection Behavior
C. Reverse Connection Verification
D. Bounce Detection Signing
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.



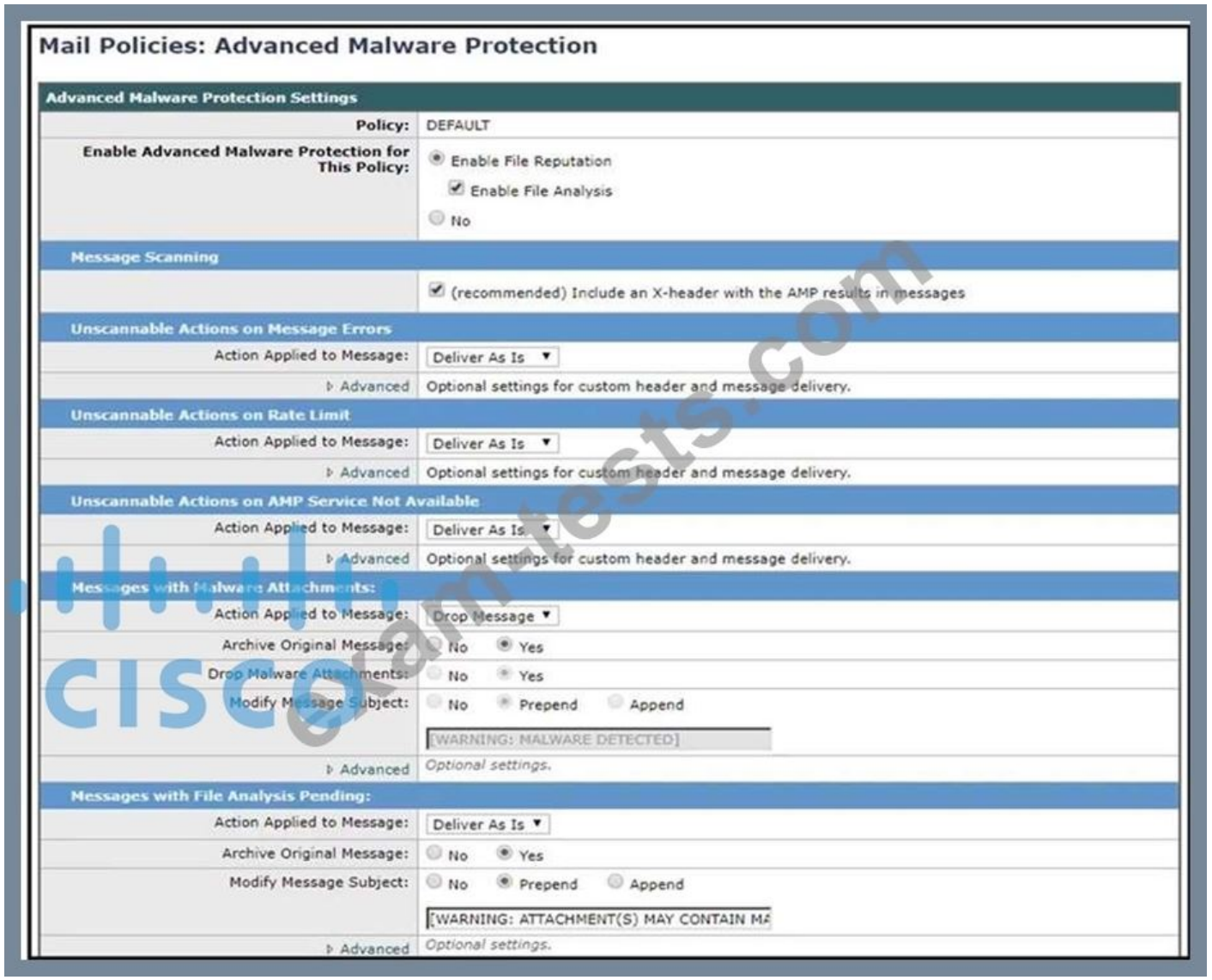
Answer:



NEW QUESTION: 25
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)
Reference:
https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scan-behavior- impact-on-av/td-p/3923243

NEW QUESTION: 26
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)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118220-technote- esa-00.html

NEW QUESTION: 27



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

A. Configure mailbox auto-remediation.

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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 created.

Which mail policy should be created to accomplish this task?

A. Outgoing Mail Flow Policy

B. Preliminary Mail Policy

C. Outgoing Mail Policy

D. Incoming Mail Flow Policy

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
An organization wants to use its existing Cisco ESA to host a new domain and enforce a separate corporate policy for that domain.
What should be done on the Cisco ESA to achieve this?
A. Use the dsestconf command to add a separate destination for the new domain.
B. Use the deli very config command to configure mail delivery for the new domain.
C. Use the smtproutes command to configure a SMTP route for the new domain.
D. Use the altrchost command to add a separate gateway for the new domain.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
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)
Explanation/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: 31
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. message action into an incoming or outgoing content filter
D. message action to take when the policy is reject/quarantine
E. ESA listeners to use the verification profile
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 32

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 commands to set filter 2 to active?

A. filters-> modify-> All-> Active

B. filters-> edit-> 2-> Active

C. filters-> set-> 2-> 1

D. filters-> detail-> 2-> 1

Answer: (SHOW ANSWER)

NEW QUESTION: 33

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

A. senderbase reputation filtering

B. NetFlow

C. heuristic-based filtering

D. geolocation-based filtering

E. content disarm and reconstruction

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 34

How does the graymail safe unsubscribe feature function?

A. It strips the malicious content of the URI before unsubscribing.

B. It checks the URI reputation and category and allows the content filter to take an action on it.

C. It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.

D. It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.

Answer: D (LEAVE A REPLY)

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200383-Graymail- Detection-and-Safe-Unsubscribin.html

NEW QUESTION: 35

What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

A. 443

B. 80

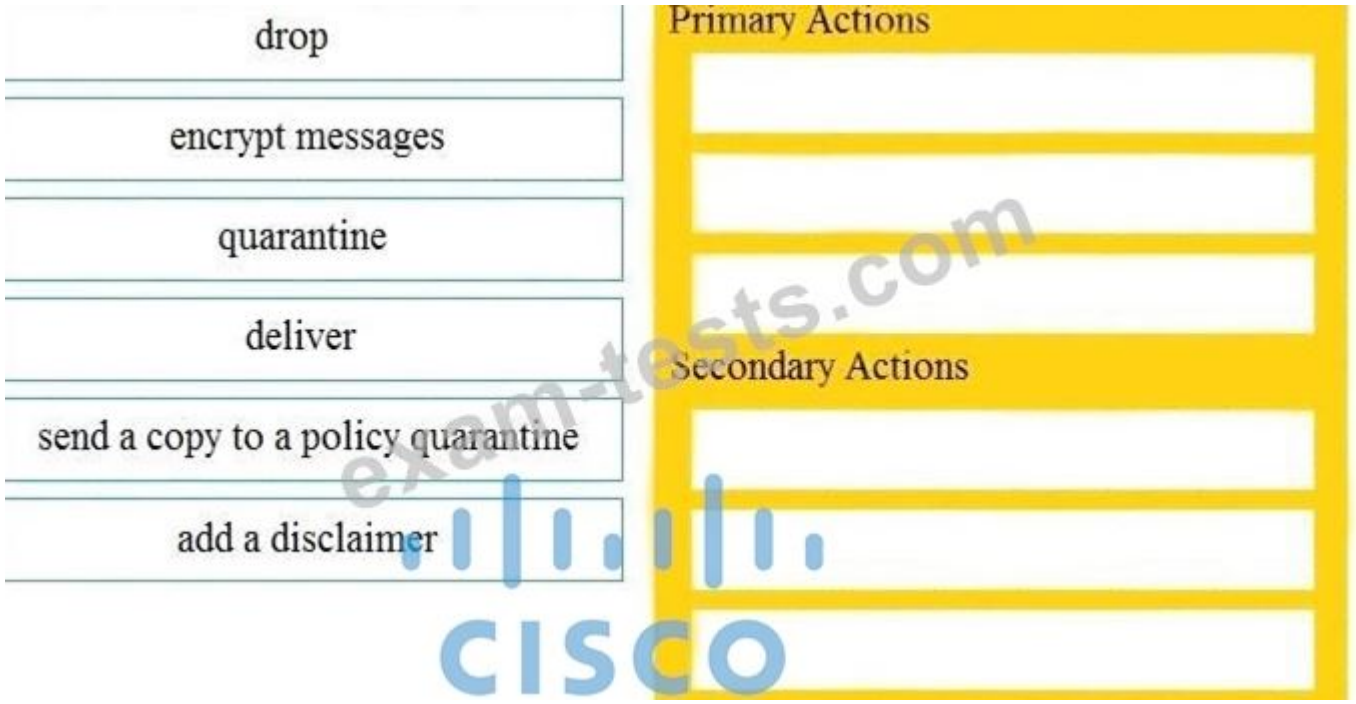
C. 82

D. 83

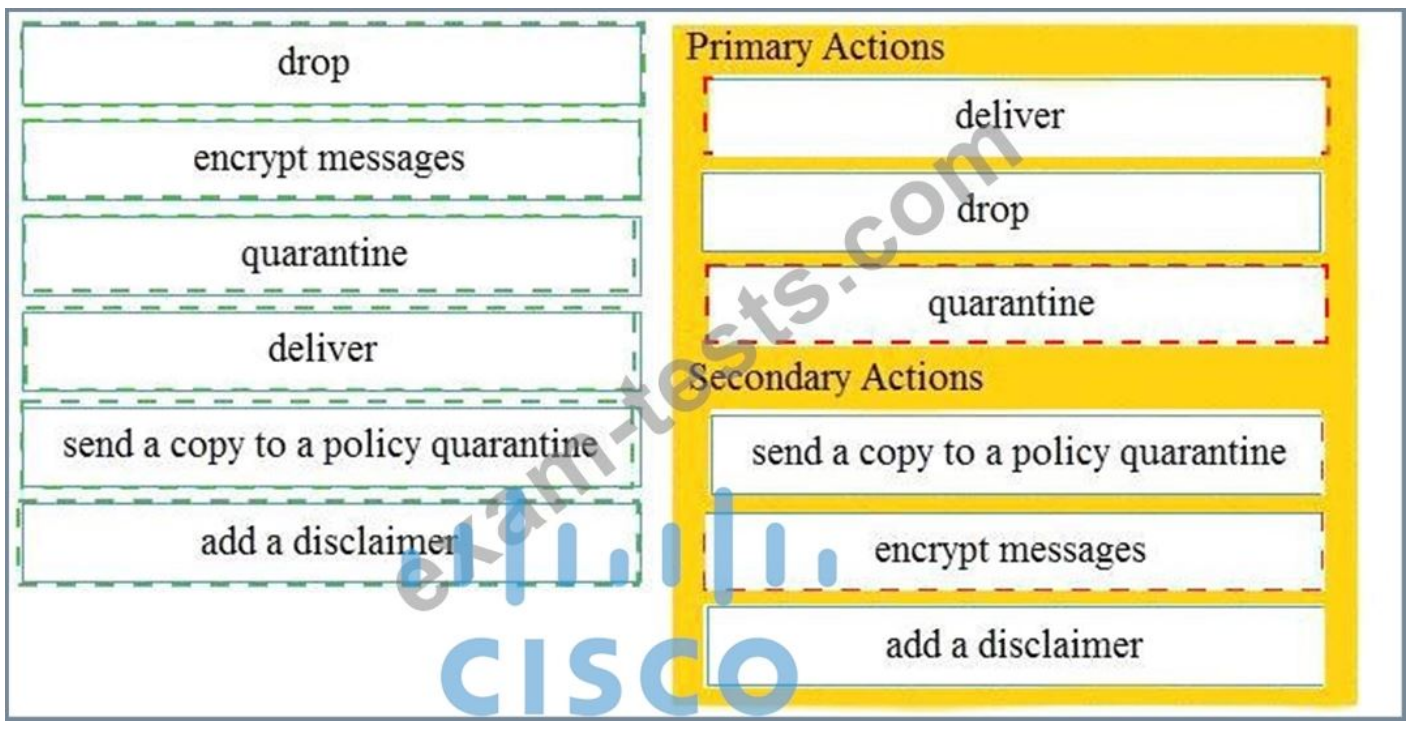
Answer: D (LEAVE A REPLY)

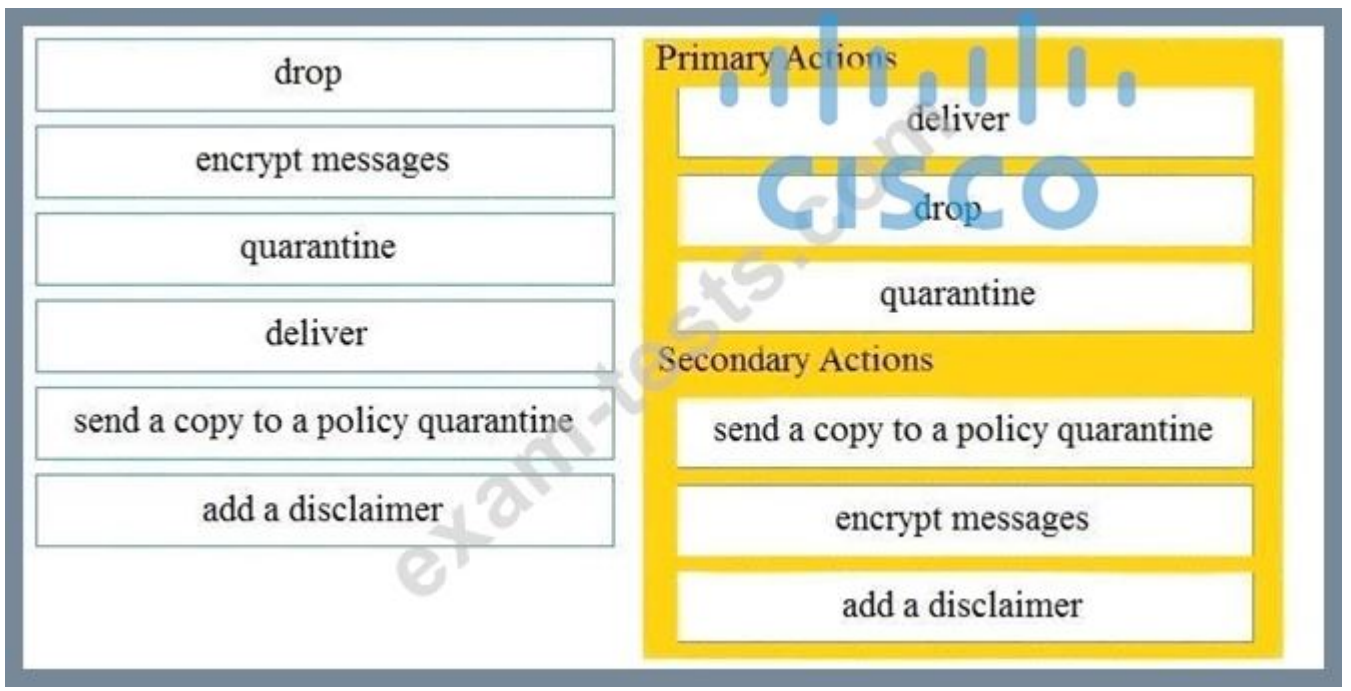
NEW QUESTION: 36

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



Answer:





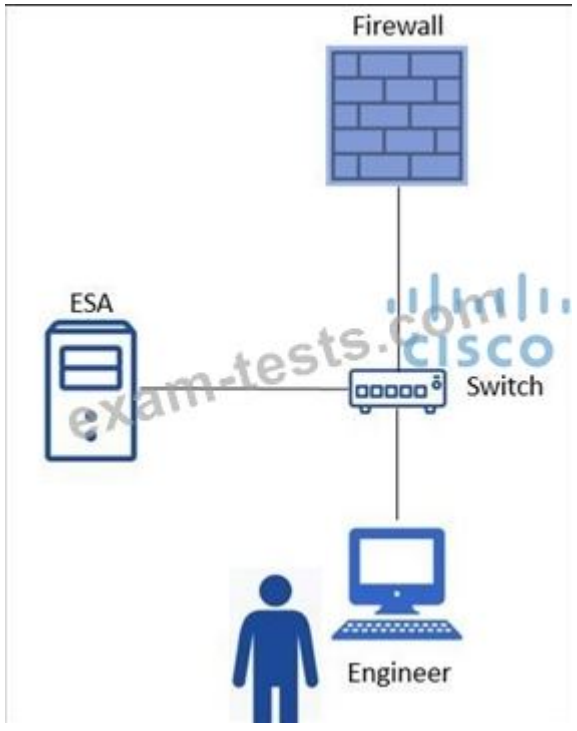
NEW QUESTION: 37
What is the default behavior of any listener for TLS communication?
A. preferred-verify
B. off
C. preferred
D. required
Answer: B (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118954-config-esa- 00.html

NEW QUESTION: 38
When email authentication is configured on Cisco ESA, which two key types should be selected on the signing profile? (Choose two.)
A. Symmetric Keys
B. DKIM
C. Public Keys
D. Domain Keys
E. Private Keys
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 39
What must be configured to allow the Cisco ESA to encrypt an email using the Cisco Registered Envelope Service?
A. provisioned email encryption profile
B. message encryption from a content filter that select "Message Encryption" over TLS
C. message encryption from the mail flow policies with "CRES" selected
D. content filter to forward the email to the Cisco Registered Envelope server
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_Admin_Guide_chapter_010010.html

NEW QUESTION: 40



Refer to the exhibit. An engineer is trying to connect to a Cisco ESA using SSH and has been unsuccessful.
Upon further inspection, the engineer notices that there is a loss of connectivity to the neighboring switch.
Which connection method should be used to determine the configuration issue?
A. Ethernet
B. HTTPS
C. serial
D. Telnet
Answer: (SHOW ANSWER)

NEW QUESTION: 41
An administrator has created a content filter to quarantine all messages that result in an SPF hardfail to review the messages and determine whether a trusted partner has accidentally misconfigured the DNS settings. The administrator sets the policy quarantine to release the messages after 24 hours, allowing time to review while not interrupting business.
Which additional option should be used to help the end users be aware of the elevated risk of interacting with these messages?
A. Notify Recipient
B. Notify Sender
C. Strip Attachments
D. Modify Subject
Answer: D (LEAVE A REPLY)

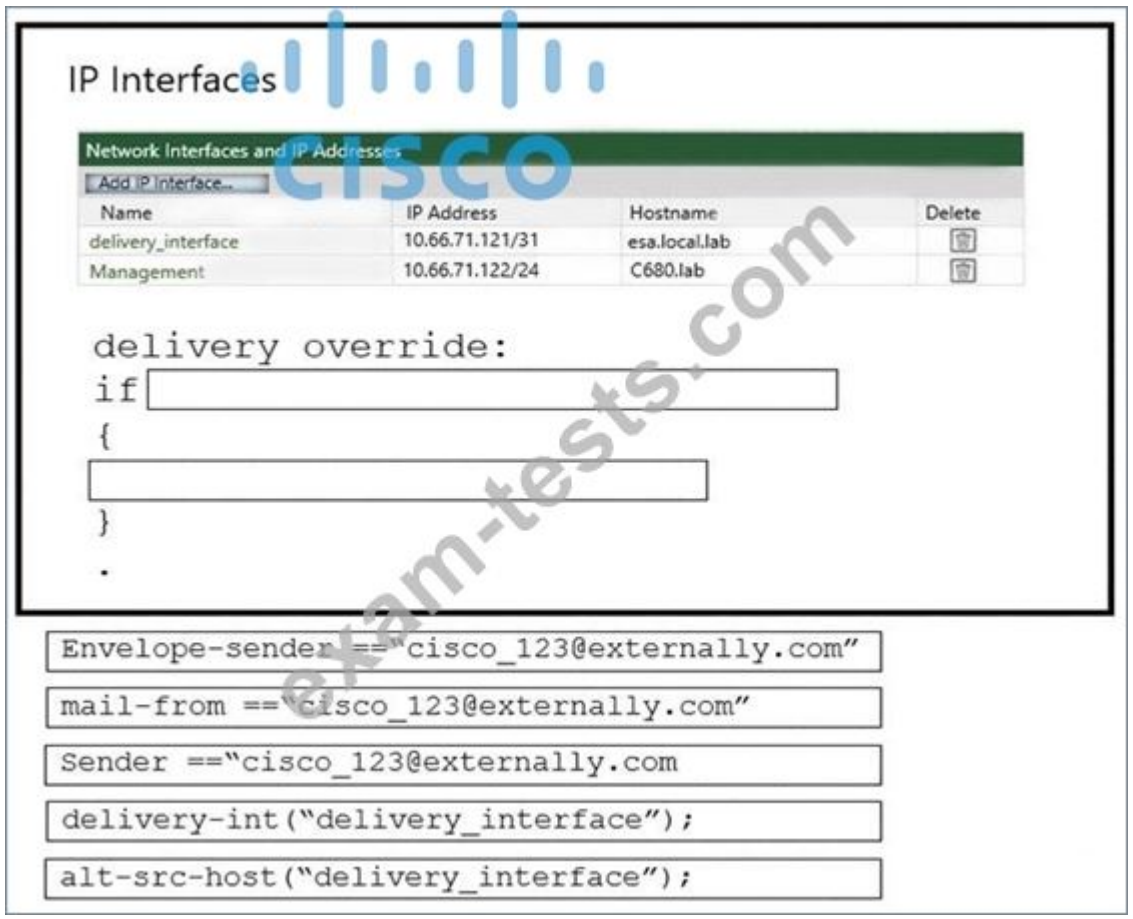
NEW QUESTION: 42
An engineer is configuring an SMTP authentication profile on a Cisco ESA which requires certificate verification.

Which section must be configured to accomplish this goal?
A. Outgoing Mail Policies
B. Verification Profiles
C. Sending Profiles
D. Mail Flow Policies
Answer: D (LEAVE A REPLY)

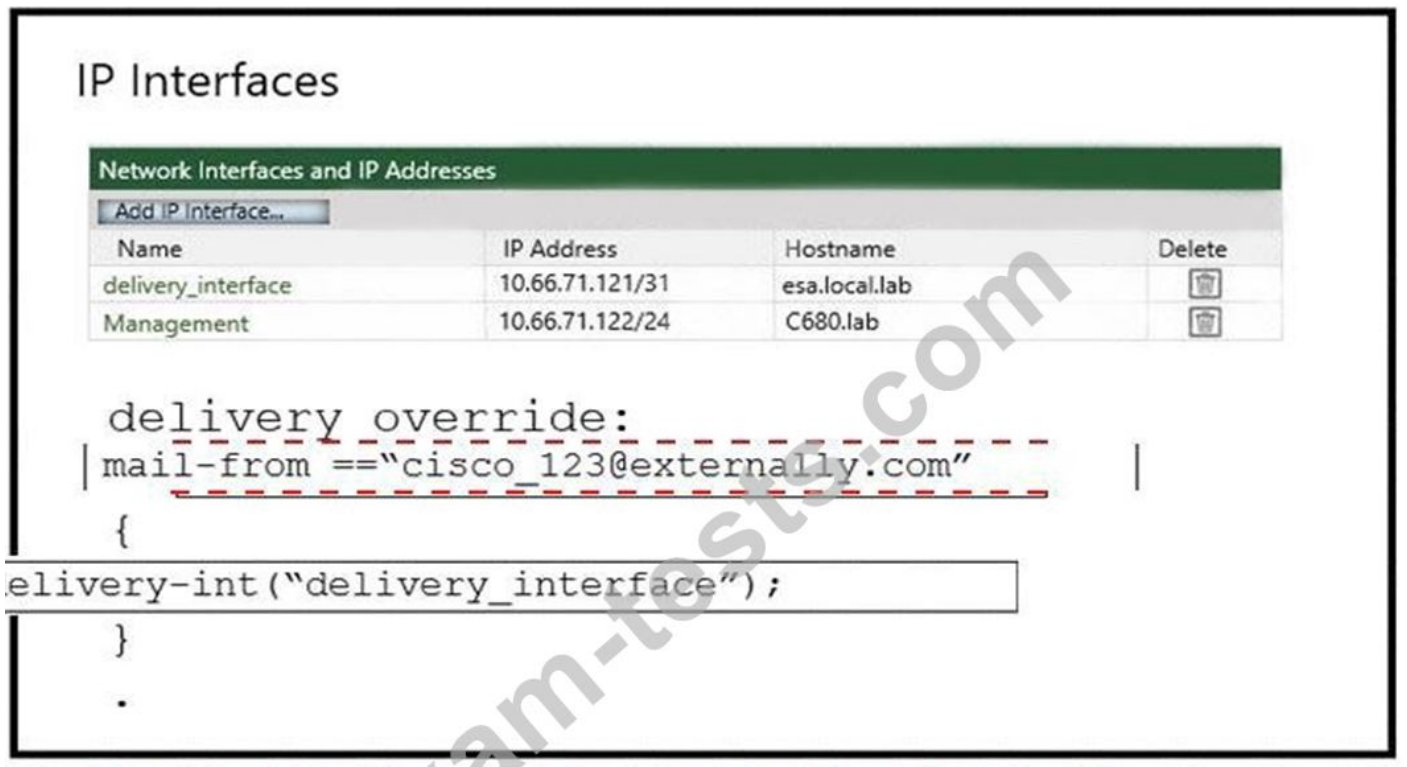
NEW QUESTION: 43
A Cisco ESA administrator has noticed that new messages being sent to the Centralized Policy Quarantine are being released after one hour. Previously, they were being held for a day before being released.
What was configured that caused this to occur?
A. The threshold settings were set to override the clock settings.
B. The retention period was changed to one hour.
C. The threshold settings were set to default.
D. The retention period was set to default.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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: A,D (LEAVE A REPLY)
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: 45
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.


IP Interfaces
Network Interfaces and IP Addresses
Add IP Interface...
Name
IP Address
Hostname
Delete
delivery_interface
10.66.71.121/31
esa.local.lab
Management
10.66.71.122/24
C680.lab
delivery override:
if
{
}
.
Envelope-sender ==“cisco_123@externally.com”
mail-from ==“cisco_123@externally.com”
Sender ==“cisco_123@externally.com
delivery-int(“delivery_interface”);
alt-src-host(“delivery_interface”);

Answer:




```
Envelope-sender ==“cisco_123@externally.com”
mail-from ==“cisco_123@externally.com”
Sender ==“cisco_123@externally.com
delivery-int(“delivery_interface”);
alt-src-host(“delivery_interface”);
```

Explanation

Table Description automatically generated

NEW QUESTION: 46

What is a benefit of implementing URL filtering on the Cisco ESA?
A. removes threats from malicious URLs
B. blacklists spam
C. provides URL reputation protection
D. enhances reputation against malicious URLs
Answer: C (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote- esa-00.html

NEW QUESTION: 47
Which benefit does enabling external spam quarantine on Cisco SMA provide?
A. ability to scan messages by using two engines to increase a catch rate
B. ability to back up spam quarantine from multiple Cisco ESAs to one central console
C. ability to consolidate spam quarantine data from multiple Cisco ESA to one central console
D. access to the spam quarantine interface on which a user can release, duplicate, or delete
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which component must be added to the content filter to trigger on failed SPF Verification or DKIM Authentication verdicts?
A. response
B. status
C. condition
D. parameter
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
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: B (LEAVE A REPLY)
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: 50
What is the purpose of Cisco Email Encryption on Cisco ESA?
A. to ensure privacy between Cisco ESA and MTA
B. to ensure integrity between a sender and MTA
C. to ensure anonymity between a recipient and MTA
D. to authenticate direct communication between a sender and Cisco ESA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
Which process is skipped when an email is received from safedomain.com, which is on the safelist?
A. message filter
B. antispam scanning
C. antivirus scanning
D. outbreak filter
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
Which type of attack is prevented by configuring file reputation filtering and file analysis features?
A. denial of service
B. zero-day
C. phishing
D. backscatter
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
What is a valid content filter action?
A. decrypt on delivery
B. skip antispam
C. archive
D. quarantine
Answer: (SHOW ANSWER)

NEW QUESTION: 54
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)
Explanation/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: 55
A network administrator is modifying an outgoing mail policy to enable domain protection for the organization. A DNS entry is created that has the public key.
Which two headers will be used as matching criteria in the outgoing mail policy? (Choose two.)
A. message-ID
B. sender
C. mail-from
D. from
E. URL reputation
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 56
What is the order of virus scanning when multilayer antivirus scanning is configured?
A. The default engine scans for viruses first and the McAfee engine scans for viruses second.
B. The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.
C. The McAfee engine scans for viruses first and the default engine scans for viruses second.
D. The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.
Answer: C (LEAVE A REPLY)
If you configure multi-layer anti-virus scanning, the Cisco appliance performs virus scanning with the McAfee engine first and the Sophos engine second. It scans messages using both engines, unless the McAfee engine detects a virus. If the McAfee engine detects a virus, the Cisco appliance performs the anti-virus actions (repairing, quarantining, etc.) defined for the mail policy.
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: 57
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,B (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa- 00.html (configuration summary)

NEW QUESTION: 58
What is the default HTTPS port when configuring spam quarantine on Cisco ESA?
A. 83
B. 82
C. 443
D. 80
Answer: (SHOW ANSWER)
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

NEW QUESTION: 59
When the Cisco ESA is configured to perform antivirus scanning, what is the default timeout value?
A. 120 seconds
B. 60 seconds
C. 30 seconds
D. 90 seconds
Answer: B (LEAVE A REPLY)