Exam Questions 300-720

Securing Email with Cisco Email Security Appliance (SESA)

https://www.2passeasy.com/dumps/300-720/

NEW QUESTION 1
Which benefit does enabling external spam quarantine on Cisco SMA provide?

A. ability to back up spam quarantine from multiple Cisco ESAs to one central console
B. access to the spam quarantine interface on which a user can release, duplicate, or delete
C. ability to scan messages by using two engines to increase a catch rate
D. ability to consolidate spam quarantine data from multiple Cisco ESA to one central console

Answer: D

NEW QUESTION 2
What are two phases of the Cisco ESA email pipeline? (Choose two.)

A. reject
B. workqueue
C. action
D. delivery
E. quarantine

Answer: BD

NEW QUESTION 3
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: AC

NEW QUESTION 4
DRAG DROP
Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.
Select and Place:

Associate the filter with a nominated incoming mail policy.	step 1
Configure a filter to take necessary action on SPF/SIDF verification results.	step 2
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	step 3
Test the results of message verification.	step 4
Configure a sendergroup to use the custom mail-flow policy.	step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Associate the filter with a nominated incoming mail policy.	Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.
Configure a filter to take necessary action on SPF/SIDF verification results.	Configure a sendergroup to use the custom mail-flow policy.
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	Associate the filter with a nominated incoming mail policy.
Test the results of message verification.	Configure a filter to take necessary action on SPF/SIDF verification results.
Configure a sendergroup to use the custom mail-flow policy.	Test the results of message verification.

NEW QUESTION 5
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 requeued.
B. It is sent in clear text.
C. It is dropped and an error message is sent to the sender.
D. It is encrypted by a Cisco encryption appliance.

Answer: B

NEW QUESTION 6
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: CD

NEW QUESTION 7
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: AB

NEW QUESTION 8
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: AD

NEW QUESTION 9
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: AD

NEW QUESTION 10
What occurs when configuring separate incoming mail policies?

A. message splintering
B. message exceptions
C. message detachment
D. message aggregation

Answer: A

NEW QUESTION 10
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: AE

NEW QUESTION 12
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

NEW QUESTION 15
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.

Answer: B

NEW QUESTION 19
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: D

NEW QUESTION 21
Which feature must be configured before an administrator can use the outbreak filter for nonviral threats?

A. quarantine threat level
B. antispam
C. data loss prevention
D. antivirus

Answer: B

NEW QUESTION 25
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: CE

NEW QUESTION 27
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: B

NEW QUESTION 30
DRAG DROP
Drag and drop the AsyncOS methods for performing DMARC verification from the left into the correct order on the right.
Select and Place:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 31
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: B

Explanation:
45 Which Cisco ESA security service is configured only through an outgoing mail policy?
A. antivirus
B. DLP
C. Outbreak Filters
D. AMP

NEW QUESTION 33
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: AE

NEW QUESTION 36

When URL logging is configured on a Cisco ESA, which feature must be enabled first?

A. antivirus
B. antispam
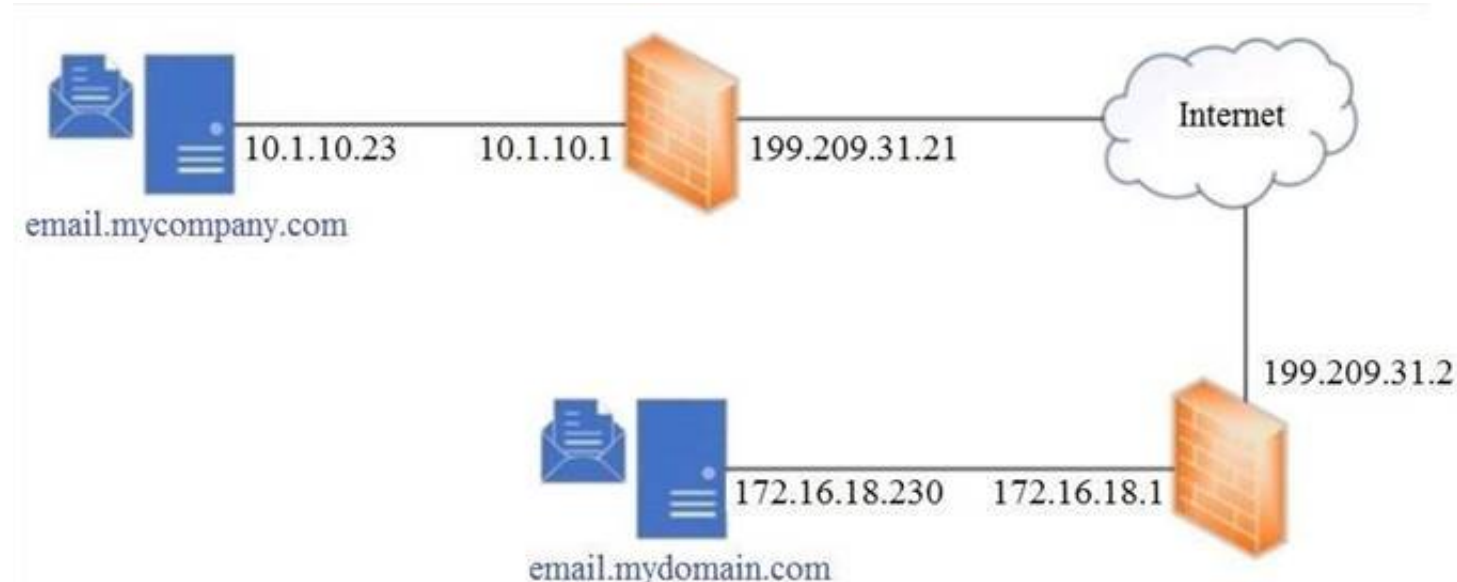C. virus outbreak filter
D. senderbase reputation filter

Answer: C

NEW QUESTION 41
What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

A. 83
B. 82
C. 443
D. 80

Answer: A

NEW QUESTION 45

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: B

Explanation:
54 What is a valid content filter action?
A. decrypt on delivery
B. quarantine
C. skip antispam
D. archive

NEW QUESTION 46
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: B

NEW QUESTION 49
What are two primary components of content filters? (Choose two.)

A. conditions
B. subject
C. content
D. actions
E. policies

Answer: AD

NEW QUESTION 53
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-720 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-720 Product From:

https://www.2passeasy.com/dumps/300-720/

Money Back Guarantee

300-720 Practice Exam Features:

* 300-720 Questions and Answers Updated Frequently

* 300-720 Practice Questions Verified by Expert Senior Certified Staff

* 300-720 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-720 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year