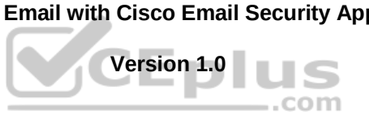
300-720.VCEplus.premium.exam.60q

Number: 300-720
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

300-720

Securing Email with Cisco Email Security Appliance



Version 1.0

Exam A

QUESTION 1

Which SMTP extension does Cisco ESA support for email security?

A. ETRN
B. UTF8SMTP
C. PIPELINING
D. STARTTLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 2 Which feature utilizes sensor information obtained from Talos intelligence to filter email servers connecting into the Cisco ESA?

A. SenderBase Reputation Filtering
B. Connection Reputation Filtering
C. Talos Reputation Filtering
D. SpamCop Reputation Filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 4 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

Correct Answer: D

Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-0/user_guide/b_SMA_Admin_Guide/b_SMA_Admin_Guide_chapter_010101.html

QUESTION 5
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

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 6 What are two phases of the Cisco ESA email pipeline?
(Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-1/user_guide/b_ESA_Admin_Guide_12_1/b_ESA_Admin_Guide_12_1_chapter_011.pdf (p.1)

QUESTION 7 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 8 Which setting affects the aggressiveness of spam detection?

A. protection level

B. spam threshold
C. spam timeout
D. maximum depth of recursion scan

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 9 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

QUESTION 10 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
Section: (none)
Explanation

Explanation/Reference:
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 11
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 12
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

Correct Answer:

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.

Section: (none)
Explanation

Explanation/Reference:
QUESTION 13 Which suboption must be selected when LDAP is configured for Spam Quarantine End-User Authentication?

A. Designate as the active query
B. Update Frequency
C. Server Priority
D. Entity ID

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-5/user_guide/b_SMA_Admin_Guide_11_5/b_SMA_Admin_Guide_11_5_chapter_01010.html

QUESTION 14 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 15
DRAG DROP

An Encryption Profile has been set up on the Cisco ESA.

Drag and drop the steps from the left for creating an outgoing content filter to encrypt emails that contains the subject "Secure:" into the correct order on the right.

Select and Place:

Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).	step 1
Submit and commit the changes.	step 2
Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.	step 3
Choose the outgoing content filters.	step 4

Correct Answer:

Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).	Choose the outgoing content filters.
Submit and commit the changes.	Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).
Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.	Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.
Choose the outgoing content filters.	Submit and commit the changes.

Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/td-p/2441383

QUESTION 16 What is the maximum message size that can be configured for encryption on the Cisco ESA?

A. 20 MB
B. 25 MBC. 15 MB
D. 30 MB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117972-technote-esa-00.html

QUESTION 17 An analyst creates a new content dictionary to use with Forged Email Detection.

Which entry will be added into the dictionary?

A. mycompany.com
B. Alpha Beta
C. ^Alpha\ Beta$
D. Alpha.Beta@mycompany.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/whitepaper_C11-737596.html

QUESTION 18
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214269-filter-to-handle-messages-that-skipped-d.html

QUESTION 19 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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
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_011010.html

QUESTION 20 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 21 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.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117863-configure-esa-00.html

QUESTION 22 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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://explore.cisco.com/esa-feature-enablement/user-guide-for-async-11

QUESTION 24 What is the default behavior of any listener for TLS communication?

A. preferred-verify
B. off
C. preferred
D. required

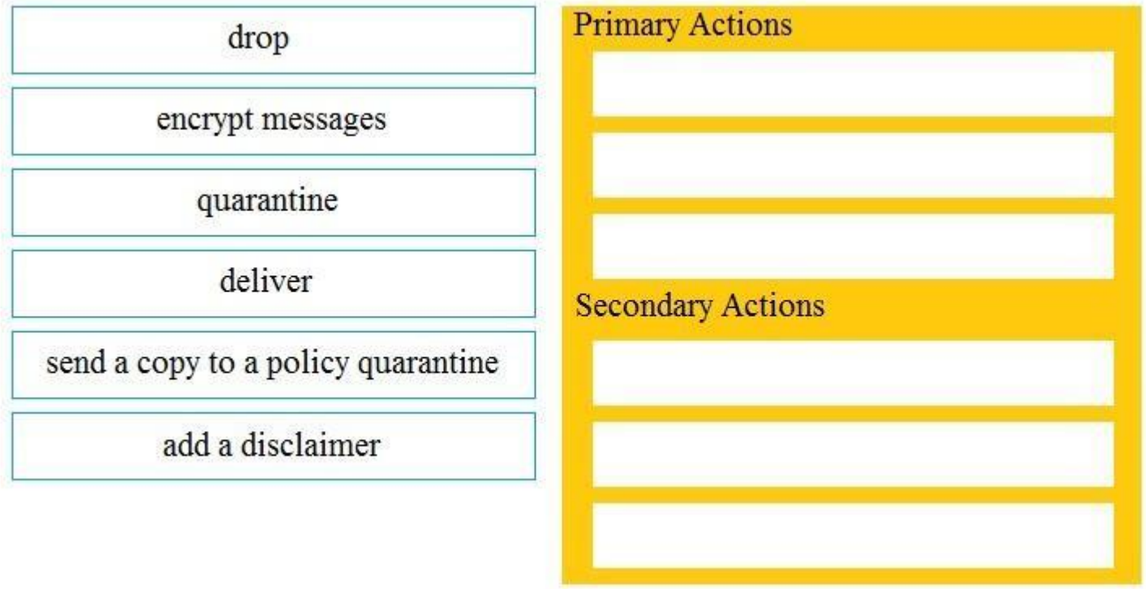
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118954-config-esa-00.html

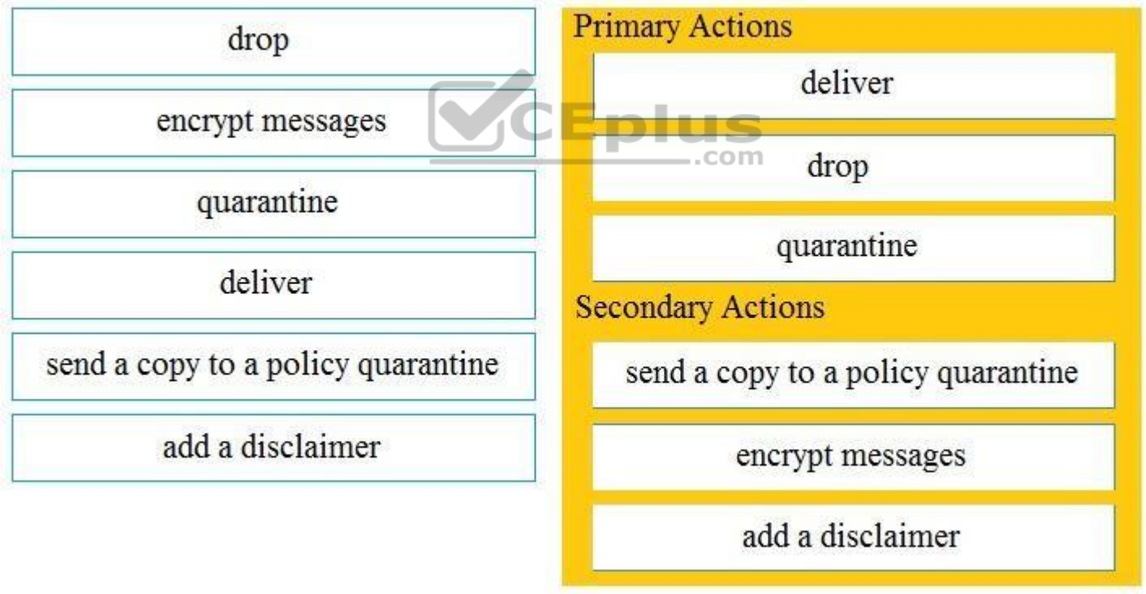
QUESTION 25
DRAG DROP

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

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
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)

QUESTION 26 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 27 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213940-esa-using-a-message-filter-to-take-act.html

QUESTION 28 What occurs when configuring separate incoming mail policies?

A. message splintering
B. message exceptions
C. message detachmentD. message aggregation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 31 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.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 32
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
Section: (none)
Explanation

Explanation/Reference:
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 33
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html

QUESTION 34 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 35 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 36 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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 37 Which attack is mitigated by using Bounce Verification?

A. spoof
B. denial of service
C. eavesdropping

D. smurf

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.networkworld.com/article/2305394/ironport-adds-bounce-back-verification-for-e-mail.html

QUESTION 38 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 39 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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 40 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 41
Which two configurations are used on multiple LDAP servers to connect with Cisco ESA? (Choose two.)

A. load balancing B.
SLA monitor
C. active-standby
D. failover
E. active-active

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can enter multiple host names to configure the LDAP servers for failover or load-balancing. Separate multiple entries with commas.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/sma_user_guide/b_SMA_Admin_Guide_ces_11/b_SMA_Admin_Guide_chapter_01010.html

QUESTION 42 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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 43
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

Correct Answer:

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.

Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 44 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**.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa-00.html (configuration summary)

QUESTION 45 Which Cisco ESA security service is configured only through an outgoing mail policy?

A. antivirus
B. DLP
C. Outbreak Filters
D. AMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 46

Which two components must be configured to perform DLP scanning? (Choose two.)

A. Add a DLP policy on the Incoming Mail Policy.
B. Add a DLP policy to the DLP Policy Manager.
C. Enable a DLP policy on the Outgoing Mail Policy.
D. Enable a DLP policy on the DLP Policy Customizations.
E. Add a DLP policy to the Outgoing Content Filter.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
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_010001.html

QUESTION 47 Which two certificate authority lists are available in Cisco ESA?
(Choose two.)

A. default
B. system
C. user
D. custom
E. demo

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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_011000.html#task_1194859

QUESTION 48 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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 49 Which two components form the graymail management solution in Cisco ESA?
(Choose two.)

A. cloud-based unsubscribe service
B. uniform unsubscription management interface for end users
C. secure subscribe option for end users
D. integrated graymail scanning engine
E. improved mail efficacy

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:
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_01101.pdf (p.2)

QUESTION 50 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html (note under enable url filtering)

QUESTION 51 What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

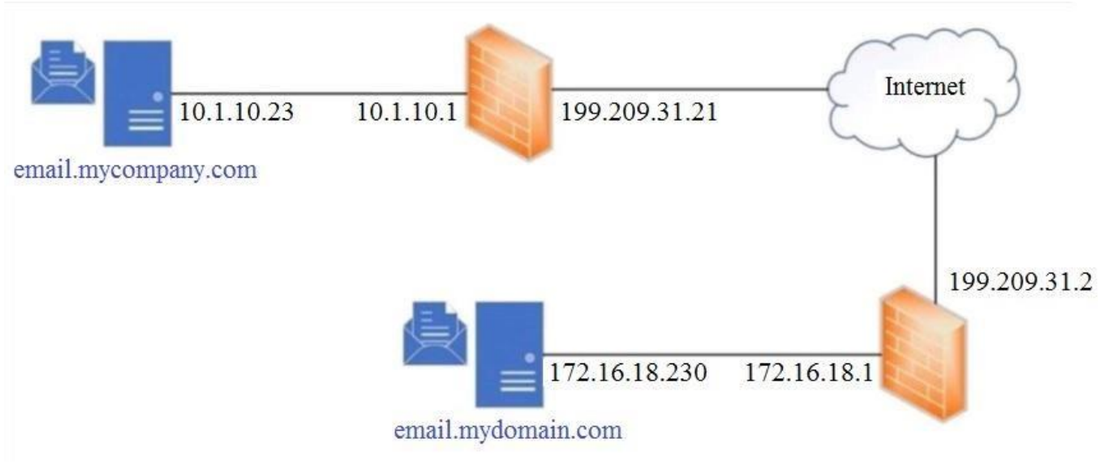
QUESTION 52 What is a benefit of implementing URL filtering on the Cisco ESA?

A. removes threats from malicious URLs
B. blacklists spam
C. provides URL reputation protection
D. enhances reputation against malicious URLs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html

QUESTION 53



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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54 What is a valid content filter action?

A. decrypt on delivery
B. quarantine
C. skip antispam
D. archive

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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_01010.html#con_1158022

QUESTION 55 When virtual gateways are configured, which two distinct attributes are allocated to each virtual gateway address? (Choose two.)

A. domain
B. IP address
C. DNS server address
D. DHCP server address
E. external spam quarantine

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118542-qa-esa-00.html

QUESTION 56 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 57 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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 58 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117922-technote-esa-00.html

QUESTION 59 Which scenario prevents a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA?

A. A policy quarantine is missing.
B. More than one email pipeline is defined.

C. The "modify the message subject" is already set.
D. The "add custom header" action is performed first.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 What are two primary components of content filters?
(Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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