Exam	**350-501**
Title	**Implementing and Operating Cisco Service Provider Network Core Technologies (350-501 SPCOR) Exam**
Version	**10.0**
Product Type	**93 Q&A with explanations**

QUESTION 1
Which SMTP extension does Cisco ESA support for email security?

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

Answer: D
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

Answer: A

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

Answer: C
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance692-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

Answer: D
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

Answer: AC
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance939-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

Answer: BD
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

Answer: AD
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

Answer: B
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance220-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.

Answer: C

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

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 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.

Answer: AC
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.

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

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.

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

Answer: A
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.

Answer: D
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.

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

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.

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

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

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

Answer: A
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance972-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

Answer: A
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

Answer: A
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance269-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

Answer: DE
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

Answer: B
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.