300-720

300-720

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

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

QUESTION 3
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

QUESTION 4
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

QUESTION 5
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

QUESTION 6
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

QUESTION 7
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

Correct Answer: A

QUESTION 8
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

QUESTION 9
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

QUESTION 10
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

QUESTION 11
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

QUESTION 12
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

QUESTION 13
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

QUESTION 14
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

QUESTION 15
What is the default behavior of any listener for TLS communication?

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

Correct Answer: B

QUESTION 16
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

QUESTION 17
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

QUESTION 18
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

QUESTION 19
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

QUESTION 20
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

QUESTION 21
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

QUESTION 22
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

QUESTION 23
Which attack is mitigated by using Bounce Verification?

A. spoof
B. denial of service
C. eavesdropping
D. smurf

Correct Answer: B

QUESTION 24
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

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

Correct Answer: CE

QUESTION 26
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

QUESTION 27
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

QUESTION 28
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

QUESTION 29
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

QUESTION 30
What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

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

Correct Answer: A

QUESTION 31
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

QUESTION 32
What is a valid content filter action?

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

Correct Answer: B

QUESTION 33
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

QUESTION 34
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

QUESTION 35
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

QUESTION 36
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