DUMPSBOSS.

Securing Email with Cisco Email Security Appliance (300-720 SESA)

Cisco 300-720

Version Demo

Total Demo Questions: 23

Total Premium Questions: 238

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco ESA Architecture and Deployment	8
Topic 2, Cisco ESA Administration	51
Topic 3, Cisco ESA Message Security	163
Topic 4, Cisco ESA Integration	16
Total	238

QUESTION NO: 1

An engineer must ensure that email sent from is not sent to the spam quarantine on a Cisco Secure Email Gateway. What must be configured on the Secure Email Gateway?

A. URL filtering

B. content filter

C. safelist

D. S/MIME

ANSWER: C

Explanation:

A safelist must be configured to ensure that messages from a trusted sender or sending domain are not treated as spam and placed in the spam quarantine. On Cisco Secure Email Gateway, safelist/blocklist entries are used to define explicit sender-based exceptions to the anti-spam process. An administrator can add a specific email address, domain, or other appropriate sender identity to the safelist, allowing mail from that source to bypass the anti-spam scanning decision that would otherwise result in quarantine. This is especially useful for known business partners, internal systems, or legitimate automated senders whose messages might resemble bulk or unsolicited mail. The safelist should be applied carefully and as narrowly as practical, because it establishes trust for the specified sender and reduces anti-spam inspection for matching messages. Cisco documents safelist and blocklist configuration as part of the appliance's anti-spam settings and mail-handling controls. See the Cisco Secure Email Gateway Administrator Guide and the Cisco Secure Email product documentation page for configuration guidance.

QUESTION NO: 2

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: A D

Explanation:

The **accept** and **route** actions can be configured on Cisco Email Security Appliance to use LDAP directory queries. An LDAP server profile defines how the appliance connects to the directory, including the server host, authentication method, search base, and query attributes. The appliance can then use directory information during SMTP processing and delivery decisions.

With **accept**, the ESA performs an LDAP recipient-acceptance query while handling the SMTP envelope. This lets the appliance validate recipient addresses against directory data and accept mail for recipients identified by the configured LDAP query. This is useful when the directory is the authoritative source for valid recipients or recipient-related attributes.

With **route**, the ESA uses an LDAP routing query to obtain delivery-routing information from directory attributes. The returned value can determine the destination mail host or route used for the message, enabling directory-driven routing for recipients, business units, or domains without maintaining every routing decision as a static appliance configuration. Cisco documents LDAP queries as supporting recipient acceptance and routing functions in ESA mail flow processing. See Cisco's ESA LDAP Queries documentation and the Cisco Email Security Appliance support documentation.

QUESTION NO: 3

Which of the following two steps are required to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance? (Choose two.)

A. Paste in the Registration Token generated from the Smart Licensing Account

B. Enable the Threat Response service under Network > Cloud Service Settings.

C. Select the correct Threat Response Server based on your region.

D. Paste in the Registration Token generated from the Security Services Exchange.

E. Enable the Security Services Exchange service under Network > Cloud Service Settings

ANSWER: B C

Explanation:

Cisco Secure Email Gateway integration with Cisco SecureX (formerly Cisco Threat Response) is configured through the appliance's cloud-service settings. The required first action is to enable the Threat Response service under *Network > Cloud Service Settings*. Enabling this service authorizes the gateway to participate in the Threat Response/SecureX integration and permits it to share the relevant observables and telemetry used for investigation and response workflows.

The administrator must also select the Threat Response Server that corresponds to the appliance's geographic region. This selection ensures that the gateway connects to the appropriate Cisco cloud endpoint for the organization's region, such as the North American, European, or Asia-Pacific service location. Together, enabling the service and choosing the regional server establish the appliance-side configuration needed for the integration. Cisco documents cloud-service and Threat Response configuration as part of Secure Email Gateway administration; see the Cisco Secure Email Gateway Administrator Guide and Cisco's Cisco Threat Response product information.

QUESTION NO: 4

An administrator needs to configure Cisco ESA to ensure that emails are sent and authorized by th e owner of the domain. Which two steps must be performed to accomplish this task? (Choose two.)

A. Generate keys.

B. Create signing profile.

C. Create Mx record.

D. Enable SPF verification.

E. Create DMARC profile.

ANSWER: A B

Explanation:

Generate keys. and **Create signing profile.** are required to configure DomainKeys Identified Mail signing on Cisco Email Security Appliance. DKIM provides domain-level message authentication: ESA signs eligible outgoing messages with a domain's private key, and receiving mail systems validate the signature by retrieving the corresponding public key from DNS. This lets recipients verify that the message was authorized by the signing domain and that signed portions of the message were not modified in transit.

Generating keys on ESA creates the cryptographic key pair used for the signing configuration. The private key remains protected on the appliance, while the generated public-key information is published by the domain administrator in a DNS TXT record under the selected DKIM selector. Creating a signing profile then associates the signing domain, selector, and generated key with ESA's outbound signing behavior. The profile is the configuration object that tells ESA which domain identity to use when applying DKIM signatures to messages. Together, key generation and a domain signing profile establish

the appliance-side DKIM configuration needed for authorized outbound mail. Cisco documents the signing-profile workflow in its ESA Administrator Guide; DKIM's signing and DNS-public-key model is defined in RFC 6376.

QUESTION NO: 5

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

A. preferred-verify

B. off

C. preferred

D. required

ANSWER: C

Explanation:

The default TLS behavior for an Email Security Appliance listener is **preferred**. In this mode, the listener advertises STARTTLS support during the SMTP exchange and attempts to negotiate TLS whenever the connecting mail server supports it. A successfully negotiated TLS session encrypts the SMTP connection, protecting the message transfer while it is in transit between the peer and the appliance.

The important operational characteristic of preferred mode is interoperability: TLS is used when available, but the listener can still accept mail from a peer that does not offer or successfully negotiate STARTTLS. This makes it an appropriate default for an Internet-facing SMTP listener, where the appliance may receive mail from many external systems with different TLS capabilities and configurations. Administrators can later apply more restrictive TLS settings when a particular mail flow requires encryption as a mandatory condition.

Cisco's ESA TLS configuration guidance describes the listener TLS modes and identifies the default listener behavior as preferred. See Cisco's Configuring TLS on Cisco ESA documentation for listener TLS configuration details.

QUESTION NO: 6

An engineer must share threat reporting information from Cisco Secure Email Gateway to Cisco SecureX. Which setting must be enabled in Secure Email Gateway?

A. SNMP

B. Security Services Exchange

C. Cloud Service Settings

D. System Monitor

ANSWER: B

Explanation:

Security Services Exchange must be enabled because it is the Cisco Secure Email Gateway integration mechanism for exchanging security telemetry and threat-related information with Cisco SecureX. In the Secure Email Gateway administration interface, this configuration establishes the appliance's connection to Cisco's security-services ecosystem so that relevant message, malware, URL, and threat-reporting data can be made available for investigation and correlation in SecureX. This integration helps analysts pivot from SecureX investigations to the email-security events and details associated with a reported threat, providing the contextual information needed for incident triage and response. The setting is specifically intended for SecureX connectivity and data sharing, so it must be configured before the gateway can participate in that workflow. Cisco documents Secure Email Gateway administration and integrations in its Secure Email Gateway Administrator Guide. Cisco's SecureX product documentation and overview also describes its role in unifying security visibility and operational workflows across integrated Cisco security products.

QUESTION NO: 7

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. Mail Flow Policies

B. Sending Profiles

C. Outgoing Mail Policies

D. Verification Profiles

ANSWER: D

Explanation:

Verification Profiles must be configured when an SMTP authentication profile needs to verify the certificate presented by the remote SMTP server. A verification profile defines the certificate-validation rules AsyncOS applies during the TLS handshake, including the trusted certificate authorities and validation behavior used to establish whether the peer certificate is acceptable. The SMTP authentication profile can then use that verification profile when it connects and authenticates to an upstream mail server over TLS.

This configuration is important because SMTP authentication credentials should be sent only after a trusted TLS connection has been established. Associating a verification profile provides the trust policy that lets the ESA validate the remote server identity rather than merely encrypting the session without validating the certificate chain and peer identity. Cisco documents verification profiles as part of its SSL/TLS certificate-validation configuration and documents SMTP authentication profiles as the location where outbound SMTP authentication settings are defined. See the Cisco Secure Email Gateway Administrator Guide and Cisco's Email Security Appliance user-guide index for the applicable AsyncOS release.

QUESTION NO: 8

Refer to the exhibit.

```
sample_filter:
if (mail-from == "test@cisco.com") AND (subject == "FW: Bounce Notification")
{
skip-viruscheck();
}
.
```

What results from this filter configuration?

A. Action is skipping all antivirus checks for the mail

B. Action is applied to all mail that has the subject "FW: Bounce Notification."

C. Action is applied to all mail from test@cisco.com.

D. Action is skipping all antispam checks for the mail.

ANSWER: A

Explanation:

Action is skipping all antivirus checks for the mail. The configured action is an antivirus-scanning bypass action, so any message that meets the filter's matching criteria is allowed to continue through mail processing without being submitted to the appliance's antivirus scanning engines. This is a message-specific processing exception: it affects the matching mail flow rather than globally disabling antivirus services on the Email Security Appliance. Such actions are available in Cisco Secure

Email message/content-filter processing to control how selected messages are handled after the defined conditions are met. In operational use, bypassing antivirus inspection should be narrowly scoped and applied only when there is a well-understood requirement, because the affected messages do not receive the malware-detection protections supplied by the enabled antivirus engines. Cisco's Email Security Appliance documentation and user-guide resources describe the available message-processing and security-policy configuration capabilities: Cisco Email Security Appliance User Guides. Cisco also provides product documentation and deployment resources for Secure Email at Cisco Secure Email.

QUESTION NO: 9 - (DRAG DROP)

An engineer must configure the message source when integrating Cisco Secure Email Threat Defense with Microsoft 365. The integration must allow visibility but not remediation. Drag and drop the actions from the left into sequence on the right to meet the requirement.

ANSWER:

Explanation:

The required sequence starts by selecting Microsoft O365 as the message source, because this identifies the Microsoft 365 tenant and mail environment that Cisco Secure Email Threat Defense will monitor. The next action is to set Microsoft 365 Authentication to Read. Read authentication is the appropriate permission mode when the goal is visibility only: Secure Email Threat Defense can obtain the message data needed for detection, investigation, and reporting, but it is not being authorized to take remediation actions against messages in the tenant.

After the source and the read-only access mode are selected, an account with Microsoft 365 Global Admin rights must sign in. This is necessary because the integration requests tenant-level application permissions, and a Global Administrator is able to provide the required organization-wide administrative consent. Once the administrator has authenticated, the final action is to accept the permissions requested for the Secure Email Threat Defense application. Accepting the consent completes the authorization process and enables the integration to read the permitted Microsoft 365 information while preserving the intended non-remediating configuration.

This flow follows the normal Microsoft identity consent model: an application first requests the selected access scope, then an authorized tenant administrator authenticates and grants consent. Microsoft documents this administrator-consent process at Grant tenant-wide admin consent to an application. The completed configuration therefore provides the required monitoring visibility while retaining read-only access.

QUESTION NO: 10

Which two message attributes can a Cisco ESA content filter evaluate? (Choose two.)

A. message headers

B. attachment file names

C. TCP window size

D. interface duplex setting

E. DNS zone serial number

ANSWER: A B

Explanation:

Message headers and **attachment file names** can be evaluated by Cisco ESA content-filter conditions. Header conditions allow a filter to match values such as From, To, Subject, or custom message headers. Attachment conditions can inspect attachment characteristics, including the file name, so that an administrator can apply handling to messages containing prohibited or sensitive file types.

Content filters combine one or more conditions with actions that determine message handling. They are configured separately for incoming and outgoing mail policies and are distinct from connection-level sender group policies. See the Cisco Secure Email Gateway Administration Guide.

QUESTION NO: 11

A recent engine update was pulled down for graymail and has caused the service to start crashing. It is critical to fix this as quickly as possible.

What must be done to address this issue?

A. Roll back to a previous version of the engine from the Services Overview page.

B. Roll back to a previous version of the engine from the System Health page.

C. Download another update from the IMS and Graymail page.

D. Download another update from the Service Updates page.

ANSWER: A

Explanation:

Roll back to a previous version of the engine from the Services Overview page. Cisco Email Security Appliance service updates, including the Graymail engine, retain a previous engine version so an administrator can quickly recover when a newly deployed engine causes operational instability. The Services Overview page is the appliance interface intended to monitor enabled security services and manage their engine versions. Selecting the affected Graymail service and rolling it back restores the previously installed engine, allowing Graymail processing to resume with the known-working version rather than waiting for a future update.

This is the appropriate immediate remediation when the timing and symptoms directly identify a recently downloaded engine as the source of service crashes. After rollback, the administrator can monitor service health and later apply a corrected engine release once it is available. Cisco documents the service-update rollback workflow under service management in the Email Security Appliance administration guidance. See the Cisco ESA Administrator Guide: Managing Service Updates and Cisco's Email Security Appliance support documentation.

QUESTION NO: 12

When the spam quarantine is configured on the Cisco Secure Email Gateway, which type of query is used to validate non administrative user access to the end-user quarantine via LDAP?

A. spam quarantine end-user authentication

B. spam quarantine alias consolidation

C. spam quarantine external authorization

D. local mailbox (IMAP/POP) authentication

ANSWER: A

Explanation:

The **spam quarantine end-user authentication** query is the LDAP query used to validate a nonadministrative user who signs in to the end-user spam quarantine. When an end user accesses the quarantine interface, Cisco Secure Email Gateway uses the configured LDAP server profile and this query to identify and authenticate the user against the organization's directory service. This enables the appliance to present quarantine contents in the context of the authenticated user rather than granting administrative-level access.

The query is configured as part of the LDAP server profile used by spam-quarantine services. It defines the directory lookup behavior needed for end-user authentication, including locating the relevant directory entry and validating credentials according to the configured LDAP authentication method. Correct configuration is essential when users access their own quarantined messages through the end-user quarantine portal, especially in environments where directory identities, email addresses, and login names may differ.

Cisco's Secure Email Gateway documentation describes LDAP server profiles and the available LDAP query types used by email and quarantine features. See the Cisco Secure Email Appliance support documentation and Cisco's Secure Email Gateway Administration Guide for LDAP and spam-quarantine configuration guidance.

QUESTION NO: 13

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: A D

Explanation:

Cisco ESA outbreak filters use the **delay** and **redirect** actions to reduce exposure while Cisco identifies and develops protection for a suspected message outbreak. The delay action temporarily holds matching mail rather than immediately delivering it. This gives Cisco Talos time to gather additional outbreak intelligence and gives the appliance an opportunity to apply updated verdicts before the message reaches the intended recipients. Delayed mail is therefore a useful protective control for rapidly evolving spam, phishing, or malware campaigns whose signatures may not yet be available at the time of initial receipt.

The redirect action sends messages matching the outbreak-filter criteria to an alternate recipient or designated mailbox. Administrators can use that destination for controlled review, analysis, or centralized handling, keeping potentially dangerous messages away from normal user inboxes while retaining a copy for investigation. Together, delaying suspicious messages and redirecting them for controlled handling provide protective containment during the period in which outbreak intelligence is being established. Cisco documents these available outbreak-filter actions and their role in controlling messages that match outbreak conditions in the Cisco ESA Advanced Phishing Protection and Outbreak Filters documentation.

QUESTION NO: 14

An engineer must integrate Cisco Secure Email with the Cisco Secure Endpoint console. Which two settings must be configured to prevent zero-day threats? (Choose two.)

A. File Reputation Filtering

B. Message Filters

C. Content Filter Settings

D. Undesirable URL Settings

E. File Analysis

ANSWER: A E

Explanation:

File Reputation Filtering and **File Analysis** are the Cisco Secure Email Advanced Malware Protection capabilities used with Cisco Secure Endpoint to protect against zero-day malware. File Reputation Filtering queries Cisco's cloud intelligence for a file's known disposition before delivery. This enables the appliance to block or quarantine files already identified as malicious and to apply policy based on reputation.

File Analysis submits eligible attachments to Cisco's analysis sandbox when their reputation is unknown or requires deeper inspection. The sandbox observes file behavior, such as exploit activity, malicious process execution, or suspicious network actions, to determine whether a previously unseen file is malicious. This behavioral analysis is central to identifying zero-day threats, because those threats may not yet have a known signature or established reputation. The resulting verdicts and file telemetry are shared through Cisco's security ecosystem, including Secure Endpoint, providing correlated visibility and retrospective protection if a file is later determined to be malicious. Cisco documents these AMP functions in the Cisco Secure Email Administration Guide and describes Secure Email's malware-defense capabilities at Cisco Secure Email.

QUESTION NO: 15

What is needed to sign outbound emails using Domain Keys Identified Mail after a signing profile is created in the Cisco Secure Email Gateway?

A. Configure in destination controls.

B. Enable DKIM in an outbound content filter.

C. Enable DKIM in the mail flow policy.

D. A signing profile referencing the sender domain is sufficient.

ANSWER: C

Explanation:

Enable DKIM in the mail flow policy. After creating a DKIM signing profile, Cisco Secure Email Gateway must be instructed when to apply that profile to messages. This is done in the applicable outgoing mail flow policy by enabling DKIM signing and selecting the signing profile. The mail flow policy is the policy-processing point that matches outbound messages according to the configured sender group, recipient group, and related message-routing criteria. Once a message matches that policy, the gateway uses the selected profile's domain, selector, and private key to generate a DKIM-Signature header before delivery.

The signing profile therefore defines the signing identity and cryptographic material, while the outbound mail flow policy activates its use for the relevant traffic. Administrators must also publish the corresponding public key as a DNS TXT record for the selector and domain defined by the profile. Receiving systems retrieve that DNS record and use it to validate the signature added by the gateway. Cisco's configuration guidance describes associating DKIM signing profiles with outgoing mail policies, and its DKIM overview explains the DNS-based verification model. See Cisco: Configure DKIM Signing on Secure Email Gateway and Cisco Email Authentication overview.

QUESTION NO: 16

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: A C

Explanation:

Cisco Email Security Appliance signing profiles support the two email-signing mechanisms represented by **DKIM** and **Domain Keys**. A signing profile associates an outbound mail domain with its signing configuration, including the selector and the cryptographic key material used to generate a signature on outgoing messages. Selecting DKIM enables standards-based DomainKeys Identified Mail signing, allowing receiving systems to retrieve the corresponding public key from DNS and validate that the message was authorized by the sending domain and has not been altered in transit.

Selecting Domain Keys supports the earlier DomainKeys signing mechanism. Cisco ESA documentation describes signing-profile configuration in terms of these two signature/key types, allowing an administrator to configure the applicable signing method for a domain and publish the matching DNS record. The private portion of the cryptographic material remains on the ESA; recipients use the published DNS information to validate the signature. This domain-associated signing process contributes to email authentication and works alongside broader sender-authentication controls such as SPF and DMARC. Cisco's configuration guidance is available in Cisco's ESA DKIM signing configuration document, and protocol details are defined by RFC 6376.

QUESTION NO: 17

Which two statements about Cisco ESA clustering are true? (Choose two.)

A. It allows shared configuration to be managed from a single machine.

B. It allows configuration changes to be committed to cluster members.

C. It creates one shared delivery queue for all members.

D. It requires all members to use the same listener IP address.

E. It automatically synchronizes local quarantine contents.

ANSWER: A B

Explanation:

A cluster allows administrators to **manage shared configuration from a single machine** and to **commit configuration changes to cluster members**. Clustered ESAs can use centralized administration so that common settings, such as mail policies and security-service configuration, are maintained consistently across appliances.

Cluster membership does not automatically create a shared delivery queue, and a cluster does not make every network interface use the same IP address. Individual appliances continue to process mail and maintain their own operational state while receiving applicable shared configuration after it is committed. Cisco documents centralized management and clustering in the Cisco Secure Email Gateway Administration Guide.

QUESTION NO: 18

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

Explanation:

`mycompany.com` is the appropriate entry because Forged Email Detection uses a content dictionary to identify domains that belong to, or are associated with, the organization being protected. Adding the organization's domain enables the Cisco Email Security Appliance to recognize messages that claim an identity related to that domain and evaluate whether the apparent sender is potentially forged. The dictionary is therefore populated with a domain value, such as the organization's primary email or web domain, rather than with a person's name, a regular-expression-style string, or a complete email address. This domain-based configuration provides the identity context that Forged Email Detection needs when inspecting sender-related information in inbound messages. Organizations can include their relevant corporate domains so the appliance can apply this detection capability consistently for those identities. Cisco describes Forged Email Detection as an anti-phishing capability designed to identify messages impersonating trusted organizational identities; proper definition of the protected organization's domain is central to that function. See Cisco's Email Security Appliance anti-phishing documentation and the Cisco Secure Email product information.

QUESTION NO: 19

An engineer must configure Directory Harvest Attack Prevention for SMTP in Cisco Secure Email Gateway. This error message must be sent when the listener receives more than 50 invalid

recipients per hour.

•500 - Too many requests

•Max. Invalid Recipients Per Hour was set to 50 already.

Which two actions must be taken next to set maximum invalid recipients per hour to meet the requirement? (Choose two.)

A. Create Max. Recipients Per Hour Code to 500.

B. Apply Max. Recipients Per Hour Text to 500 - Too many requests.

C. Configure Max. Recipients Per Hour Code to 500.

D. Set Max. Recipients Per Hour Text to Too many requests.

E. Implement Max. Recipients Per Hour Text to 500 - Too many requests.

ANSWER: C D

Explanation:

Directory Harvest Attack Prevention uses the configured maximum invalid-recipient threshold to identify excessive recipient probing on an SMTP listener. Because the threshold is already set to 50 invalid recipients per hour, the remaining configuration is the SMTP reply delivered when that threshold is exceeded. The reply is composed of two separately configured values: an SMTP response code and accompanying response text. Therefore, **Configure Max. Recipients Per Hour Code to 500.** supplies the required numeric SMTP status code, while **Set Max. Recipients Per Hour Text to Too many requests.** supplies the required human-readable reply text. Together, these settings produce the requested response, `500 Too many requests`, when the listener's invalid-recipient rate crosses the configured limit. Cisco Secure Email Gateway exposes Directory Harvest Attack Prevention settings in the SMTP listener configuration, allowing administrators to define invalid-recipient limits and the SMTP response returned after a limit is reached. Cisco's configuration guidance for SMTP listeners is available in the Cisco Secure Email Gateway User Guide. For SMTP response-code semantics, see RFC 5321, SMTP Reply Codes.

QUESTION NO: 20

An engineer must add cisco.com to the listed domains in Cisco Secure Email Gateway that accept messages. All other domains must be blocked, and the message must be sent back to the sender is Domain Blocked. Which two actions must be taken to meet the requirement? (Choose two.)

A. From the IP Reputation Filtering settings, accept Cisco com and reject all other URLs

B. From the Sender Domain Reputation Filtering settings, accept Cisco com and reject all other URLs.

C. Configure Domain blocked as a custom threat response.

D. Accept Cisco com and reject all other URLs in the Recipient Access Table.

E. Configure Domain blocked as a custom SMTP response

ANSWER: D E

Explanation:

The Recipient Access Table is the Cisco Secure Email Gateway control that determines whether the appliance accepts or rejects mail according to the recipient domain (and, where configured, recipient addresses). To meet the stated requirement, the table must include an explicit acceptance entry for `cisco.com` and a default or subsequent rejection policy for every other recipient domain. This ensures the gateway only accepts messages addressed to the authorized domain rather than making a decision based on the connecting IP address or the sender's domain reputation.

A custom SMTP response is also required because recipient-access rejection occurs during the SMTP conversation. Configuring the rejection response as `Domain Blocked` causes the sending mail server to receive that text with the SMTP rejection, thereby notifying the sender that delivery was refused under the domain policy. Cisco documents recipient acceptance and rejection as an access-policy function of the Recipient Access Table, while SMTP response customization controls the response text returned for rejected SMTP transactions. See Cisco's Email Security Appliance documentation and the Cisco Secure Email Gateway Administrator Guide.

QUESTION NO: 21

The CEO added a sender to a safelist but does not receive an important message expected from the trusted sender. An engineer evaluates message tracking on the Cisco Secure Email Gateway appliance and determines that the message was dropped by the antivirus engine. What is the reason for this behavior?

A. The sender is included in an ISP blocklist

B. Administrative access is required to create a safelist.

C. The sender didn ' t mark the message as urgent

D. End-user safelists apply to antispam engines only.

ANSWER: D

Explanation:

End-user safelists apply to antispam engines only. On Cisco Secure Email Gateway, an end user can safelist a sender or domain through the end-user quarantine or an integrated client workflow so that mail from that source is not treated as spam by the antispam service. This exception is deliberately limited in scope: it changes the antispam verdict handling for the listed sender and does not establish a general bypass for every mail-security control on the appliance.

Antivirus scanning remains active because it protects recipients from malware that can arrive even from a known, trusted, or previously legitimate sender. A trusted sender account may be compromised, or a message may contain an infected attachment, so allowing a user safelist to override the antivirus engine would create a significant security exposure. Therefore, message tracking can correctly show that the sender was safelisted for antispam purposes while the same message was still scanned and dropped based on its antivirus result. Cisco documents the end-user safelist capability and

its antispam-specific behavior in its Secure Email Gateway guidance: Cisco Secure Email Gateway Safelists and Blocklists documentation. See also Cisco's overview of the platform's layered email defenses at Cisco Secure Email.

QUESTION NO: 22

Refer to the exhibit.

An administrator has configured File Reputation and File Analysis on the Cisco Secure Email Gateway appliance however it does not function as expected What must be configured on the appliance for this to function?

A. Upload the Root CA certificate for the File Reputation cloud to the Cisco Secure Email Gateway.

B. Open port 443 on the firewall for the Cisco Secure Email Gateway to connect to the File Reputation cloud.

C. Configure the Cisco Secure Email Gateway to use SSL for the connection to the File Reputation server

D. Restart the File Reputation service to force the scanning engine to connect to the File Reputation cloud.

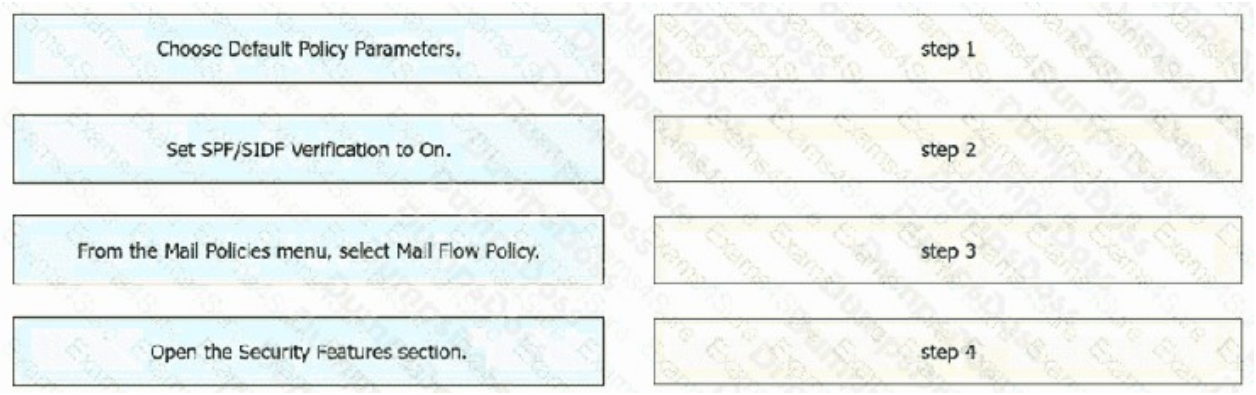
ANSWER: B

Explanation:

Open port 443 on the firewall for the Cisco Secure Email Gateway to connect to the File Reputation cloud. File Reputation and File Analysis depend on the Secure Email Gateway being able to initiate outbound HTTPS connections to Cisco's cloud-based analysis infrastructure. The appliance sends file reputation lookups and, when policy and analysis requirements call for it, submits supported files or retrieves analysis results through this secure cloud connection. If the network firewall blocks outbound TCP port 443, the configured scanning features cannot communicate with the cloud service and therefore cannot return reputation or file-analysis verdicts as expected. HTTPS already provides the required transport security for these service interactions; the operational requirement is to permit the appliance's outbound connectivity to the Cisco cloud endpoints. Administrators should ensure that the firewall policy allows the appliance to establish and maintain these outbound HTTPS sessions, including any required return traffic, and should validate connectivity from the appliance after the rule is applied. Cisco's Secure Email Gateway documentation describes File Analysis as a cloud-connected service and lists network connectivity prerequisites in its configuration guidance. See the Cisco Secure Email Gateway Administrator Guide and Cisco's Secure Email product documentation.

QUESTION NO: 23 - (DRAG DROP)

Drag and drop the actions from the left into sequence on the right to validate the authenticity of email on a Cisco Secure Email Gateway by using DNS records.



ANSWER:

Explanation:

To enable DNS-based sender-authenticity validation on a Cisco Secure Email Gateway, begin in **Mail Policies** and select **Mail Flow Policy**. Mail flow policies control how the appliance evaluates and handles messages as they pass through the

system. The default mail flow policy is the appropriate policy to edit when the requested validation behavior is intended to apply broadly to mail processed by the gateway.

Next, choose **Default Policy Parameters**. This opens the configuration settings associated with that policy rather than merely displaying the list of available policies. Within the policy parameters, open the **Security Features** section. Cisco places sender-validation controls in this section because they are security checks applied during message processing.

Finally, set **SPF/SIDF Verification** to **On**. When this verification is enabled, the gateway performs DNS lookups for the sending domain's published Sender Policy Framework information and evaluates whether the connecting sender is authorized by that domain's policy. This lets the appliance use domain-published DNS records as part of its authenticity assessment before applying the configured mail-flow handling. Cisco's documentation describes SPF verification as a DNS-based mechanism used to validate authorized sending hosts and documents these policy-level security settings in the mail-flow configuration workflow. See Cisco's Secure Email Gateway User Guide and the Cisco Secure Email Gateway configuration guides for the relevant administrative configuration context.