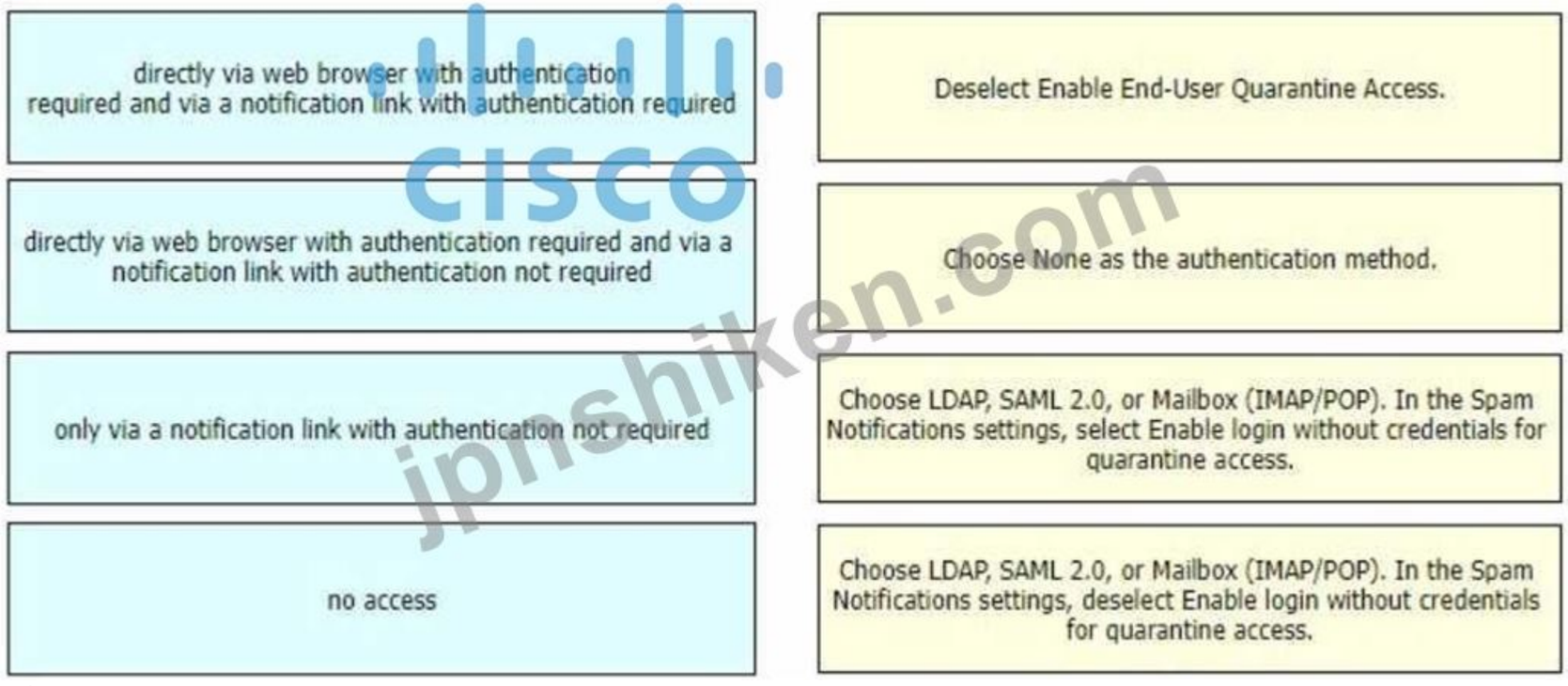
Cisco.300-720J.v2026-08-13.q111

試験コード：	300-720J
試験名称：	Securing Email with Cisco Email Security Appliance (300-720日本語版)
認証ベンダー：	Cisco
無料問題の数：	111
バージョン：	v2026-08-13
ページの閲覧量：	104
問題集の閲覧量：	1165

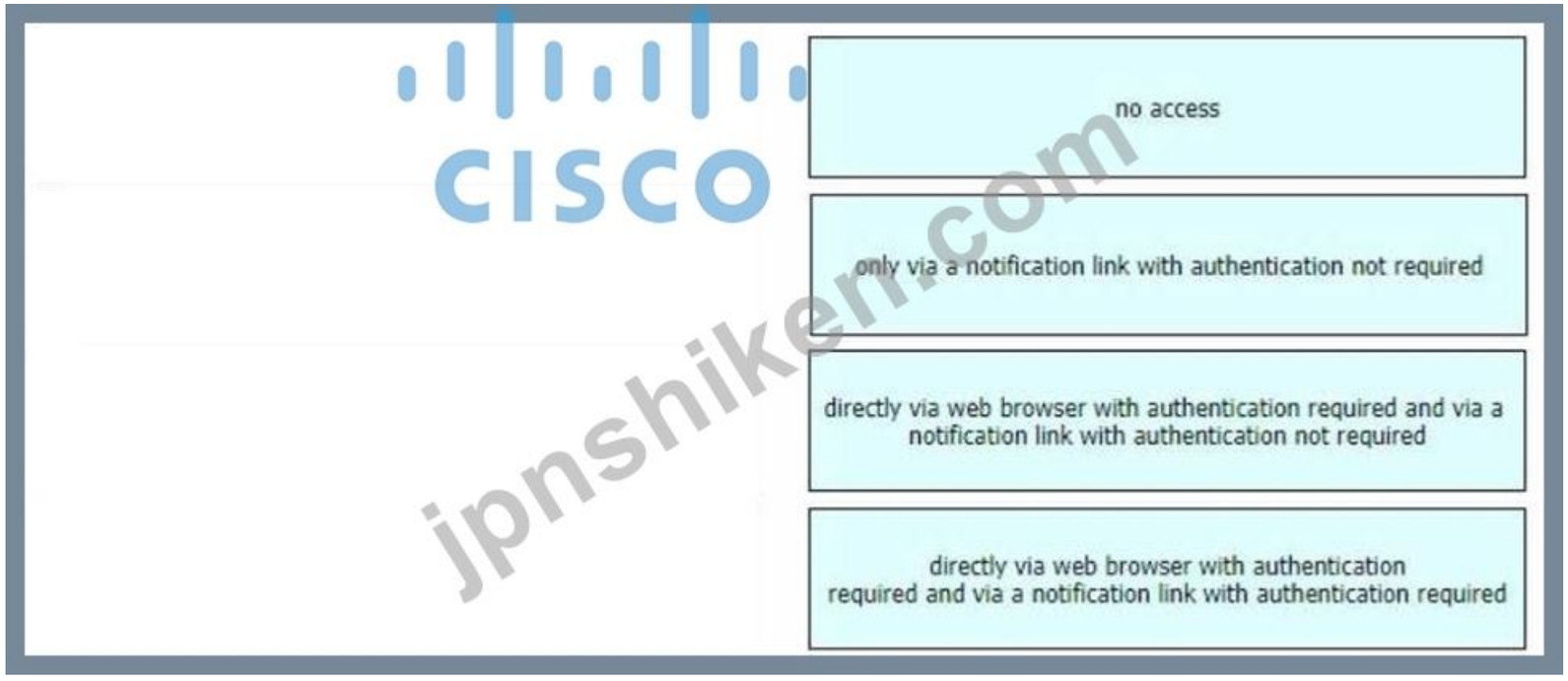
https://www.jpnshiken.com/shiken/Cisco.300-720J.v2026-08-13.q111.html

質問: **1**
エンジニアはオンプレミスのCisco Secure Email Gatewayを導入する必要があります。Secure Email Gatewayをネットワークに物理的に接続した後、以下の設定を行います。
システムセットアップウィザードを実行します。
- Active Directoryウィザードを実行します。
ネットワーク設定を構成します。
Cisco Secure Email Gatewayがホワイトリスト、ブラックリスト、およびグレーリストを更新する際に、送信者ベースの評判スコアを照会できるようにするには、どの設定が必要ですか？
A. 外部脅威フィード機能のキーを取得します。
B. Cisco Notificationサービスを設定します。
C. レポート機能を有効にします。
D. メッセージ追跡サービスを設定します。
正解: **B** (コメントを発表する)
The Cisco Notification service must be configured so the Cisco Secure Email Gateway can communicate with Cisco cloud services, including SenderBase/Talos reputation services used to query sender reputation information for sender-group list updates.

質問: **2**
ドラッグアンドドロップ問題
エンドユーザー隔離アクセス用の認証オプションを、左側から右側の対応する設定手順にドラッグ＆ドロップしてください。



正解:



Explanation:

End-user quarantine access is controlled by authentication options. LDAP, SAML, or IMAP/POP enforce authentication; enabling login without credentials allows link-based access; choosing None bypasses authentication; disabling end-user access removes quarantine visibility completely.

質問: **3**
Cisco ESAでメールエイリアス宛てのスパムメッセージを確認する際に考慮すべき点は何ですか？
A. 通知内のリンクからのみ可能です。
B. ウェブブラウザ経由で直接アクセスする場合のみ可能です。
C. アクセスはあらゆる方法で許可されます。
D. メールボックス認証では不可能です。
正解: **D (コメントを発表する)**
Authentication Options for End Users Accessing Spam Management Features Note Mailbox authentication does not allow users to view messages addressed to an email alias.
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_011111.html?bookSea rch=true

質問: **4**
管理者がウイルス以外の脅威にアウトブレイクフィルターを使用する前に、どの機能を設定する必要がありますか？
A. 隔離脅威レベル
B. スパム対策
C. データ損失防止
D. ウイルス対策
正解: **(正解を表示します)**
By default, the Outbreak Filters feature scans your incoming and outgoing messages for possible viruses during an outbreak. You can enable scanning for non-viral threats in addition to virus outbreaks if you enable anti-spam scanning on the appliance.
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

質問: **5**
クライアント証明書を使用してSMTPセッションを認証する機能は何ですか？
A. セキュアメールゲートウェイは、アプライアンスへの接続時に、ユーザーのメールクライアントからクライアント証明書を要求します。
B. セキュアメールゲートウェイが、メール送信時にユーザーに証明書の提供を要求するように設定されている場合、いかなるユーザーに対しても例外は認められません。
C. ユーザーは、安全な SSL 接続を介してメッセージを送信し、アプライアンスからのサーバー証明書を受け入れるようにメール クライアントを設定する必要があります。
D. 証明書が有効な場合、セキュアメールゲートウェイはメールクライアントからのTLS経由のSMTP接続を許可します。
正解: **(正解を表示します)**
When authenticating SMTP sessions using client certificates, the Cisco Secure Email Gateway validates the client's certificate. If the certificate is valid, the gateway permits the SMTP connection over TLS, ensuring secure and authenticated mail delivery.

質問: **6**
Cisco ESAがCisco Security Management Appliance上でメッセージを隔離するために使用するデフォルトポートはどれですか？
A. ポート4766/UDP
B. ポート110/TCP
C. ポート6025/TCP
D. ポート25fTCP
E. ポート443/TCP
正解: **C (コメントを発表する)**

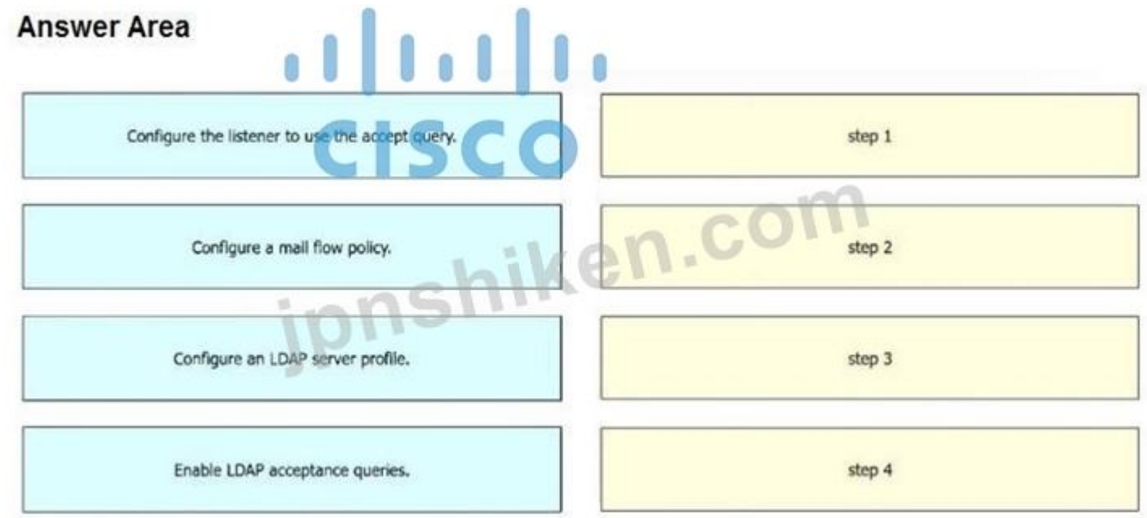
質問: **7**
Talosのインテリジェンスから取得したセンサー情報を利用して、Cisco ESAに接続する電子メールサーバーをフィルタリングする機能はどれですか。
A. SenderBaseレピュテーションフィルタリング
B. 接続レピュテーションフィルタリング
C. Talosレピュテーションフィルタリング
D. SpamCopレピュテーションフィルタリング
正解: **(**正解を表示します**)**
SenderBase Reputation Filtering is a feature that allows Cisco ESA to reject or throttle connections from email servers based on their reputation score, which is calculated by Talos using sensor information from various sources.

質問: **8**
TLS通信のリスナーのデフォルトの動作は何ですか？
A. 優先確認
B. オフ
C. 優先
D. 必須
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118954-config-esa-00.html

質問: **9**
セキュリティエンジニアは、info@partners.com からの正当なメールが Cisco Secure Email でスパムとして隔離されないようにしたいと考えています。
この要件を満たすためには、どのような措置を講じる必要がありますか？
A. ブロックリストからドメインを削除します。
B. ドメインを許可リストに追加します。
C. ドメインをセーフリストに追加します。
D. partners.com のすべてのメールアドレスを許可リストに追加します。
正解: **C (**コメントを発表する**)**
Adding the sender to the safelist ensures legitimate messages from that address bypass spam quarantine handling in Cisco Secure Email.

質問: **10**
以下のDNSレコードのうち、特定のドメインのメール配信を扱うものはどれですか？
A. TXT
B. A
C. PTR
D. MX
正解: **(**正解を表示します**)**

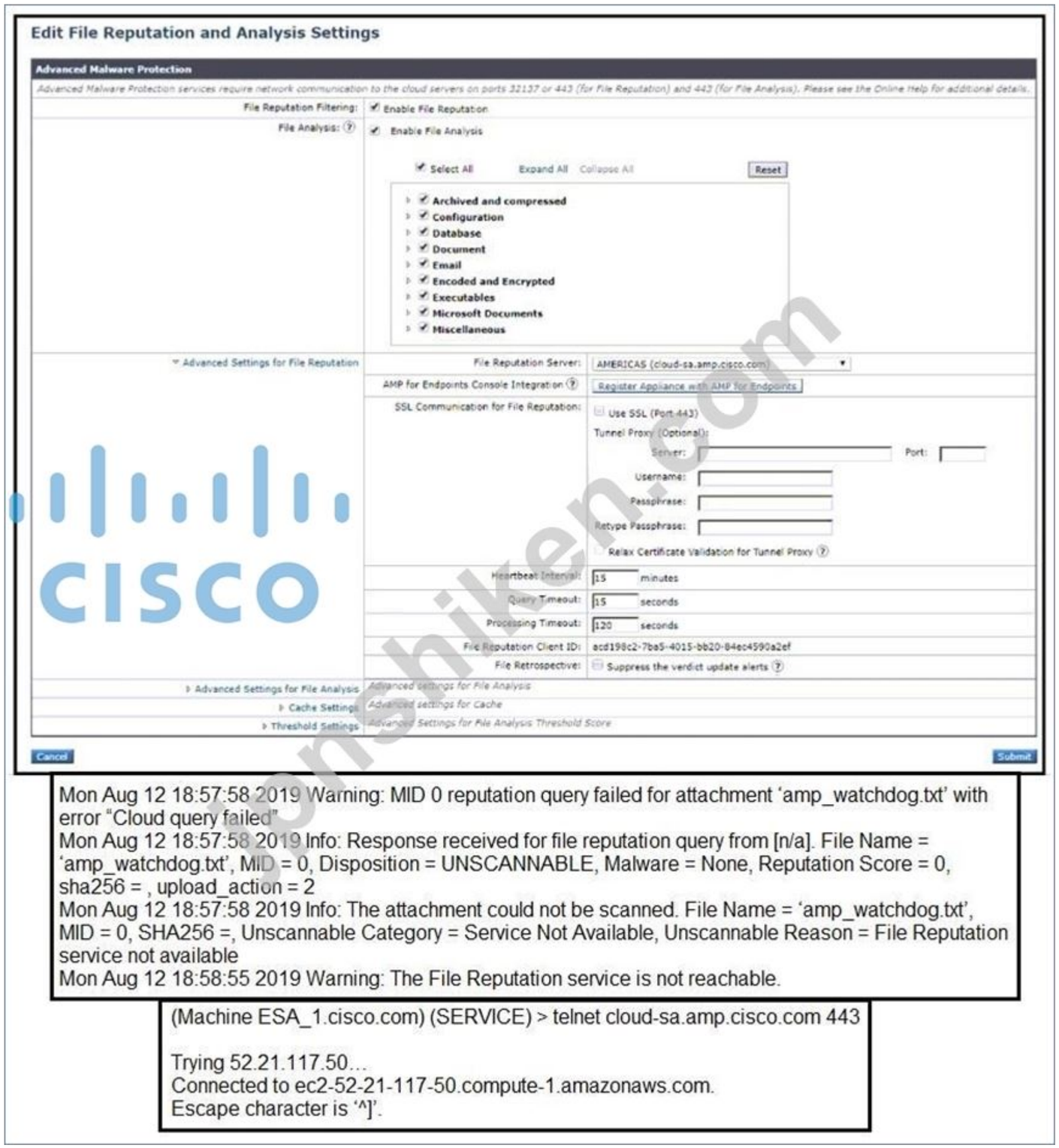
質問: **11**
ドラッグアンドドロップ問題
Cisco Secure Email Gateway でディレクトリ収集防止を設定するには、左側のアクションを右側のシーケンスにドラッグアンドドロップします。



正解:

Explanation:
You first define the LDAP server profile, enable the necessary LDAP queries, configure the listener to use those queries, and finally apply policies to control how mail is handled for recipient validation and directory harvest prevention.

質問: **12**
図を参照してください。管理者がCisco ESA上でファイルレピュテーションとファイル分析を設定しましたが、期待どおりに動作しません。
この機能を実現するには、Cisco ESAでどのような設定が必要ですか？



A. ファイルレピュテーションクラウドのルートCA証明書をCisco ESAにアップロードします。

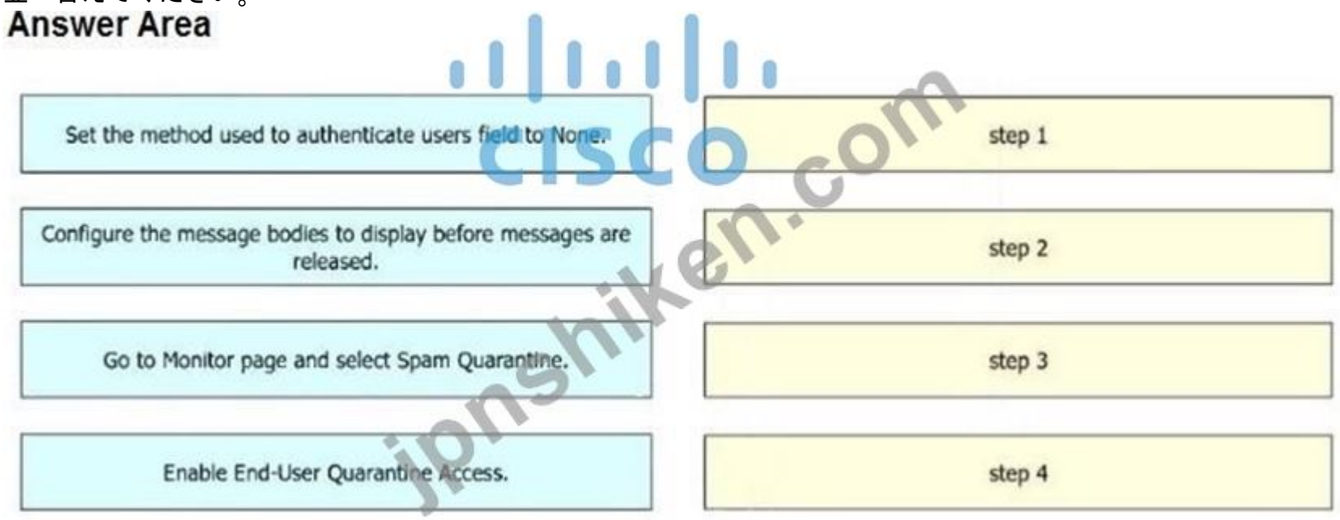
B. Cisco ESAがファイルレピュテーションクラウドに接続できるように、ファイアウォールでポート443を開放します。

C. ファイルレピュテーションサービスを再起動して、スキャンエンジンがファイルレピュテーションクラウドに接続するように強制します。
D. Cisco ESA を設定して、ファイル レピュテーション サーバーへの接続に SSL を使用するようにします。
正解: **(**正解を表示します**)**
In the example the SSL checkbox is not marked yet, and it shows that the ESA is able to telnet on port 443 so port must be open.

質問: **13**
エンジニアは、Cisco Secure Email Gateway でドメインベースメッセージ認証、レポート、および適合性 (DMARC) を有効にする必要があります。DMARC 検証に失敗したメッセージは、SMTP コード 550 を使用して、以下の応答で拒否する必要があります。
#5.7.1 DMARC認証なしのメールは禁止されています。
DMARC検証プロファイルを作成した後、どのような操作を行う必要がありますか？
A. 隔離された DMARC レコードでポリシーを適用すると、AsyncOS はレコードを隔離する必要があります。
B. 隔離された DMARC レコードでポリシーを設定すると、AsyncOS はレコードを拒否する必要があります。
C. DMARC検証中にメッセージが一時的に失敗した場合、AsyncOSはレコードを拒否する必要があります。
D. 拒否された DMARC レコードでポリシーを実装すると、AsyncOS はレコードを拒否する必要があります。
正解: **D (**コメントを発表する**)**
After creating the DMARC verification profile, the administrator must apply a DMARC policy action for domains whose DMARC record specifies reject. Configuring AsyncOS to reject those failed messages enforces the sender domain's DMARC policy and allows the appliance to return the required SMTP 550 response.

質問: **14**
ドラッグアンドドロップ問題
エンジニアは、Cisco Secure Email Gateway 上のスパム隔離へのユーザーアクセス権限を付与する必要があります。ユーザーは、リンクを使用して追加の認証なしにスパム隔離にアクセスできる必要があります。また、スパム隔離セクション内でスパムメッセージを復元することなくプレビューできる必要があります。要件を満たすように、左側のアクションを右側にドラッグアンドドロップして順番に並べ替えてください。

Answer Area



正解:

Answer Area

Go to Monitor page and select Spam Quarantine.

Enable End-User Quarantine Access.

Set the method used to authenticate users field to None.

Configure the message bodies to display before messages are released.

Explanation:
You begin by navigating to the Spam Quarantine settings, enable user access, configure authentication to None for link-based access, and then set up message preview for users.

質問: **15**
送信者に基づいて電子メール配信を制御するために使用される2つのCiscoESA機能はどれですか。 2つ選択してください。）
A. 受信メールポリシー
B. スパム検疫
C. アウトブレイクフィルター
D. セーフリスト
E. ブロックリスト
正解: **(**正解を表示します**)**
Using Safelists and Blocklists to Control Email Delivery Based on Sender.
Administrators and end users can use safelists and blocklists to help determine which messages are spam. Safelists specify senders and domains that are never treated as spam. Blocklists specify senders and domains that are always treated as spam.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_0100000.html?bookSearch=true#con_1624156

質問: **16**
ある組織では、複数のCisco ESAデバイスを導入しており、その結果、管理すべきスパム隔離領域が複数存在します。隔離されたメッセージを管理するために、管理者はCisco SMAで集中型スパム隔離を有効にし、Cisco ESAデバイスで外部スパム隔離を設定しました。しかし、メッセージは依然としてCisco ESAデバイスのローカル隔離領域に送られています。設定を完了するには、どのような変更が必要ですか？

A. Cisco ESA デバイスの受信メール ポリシーを変更して、外部隔離にリダイレクトします。
B. Cisco ESA デバイスで外部スパム隔離を無効にします。
C. Cisco ESA デバイスでローカル スパム隔離を無効にします。
D. Cisco ESA デバイスの外部スパム隔離設定を変更し、ポートを次のように変更します。
25.
正解: (正解を表示します)
To use the centralized spam quarantine on the Cisco Secure Email and Web Manager appliance, the administrator must disable the local spam quarantine on the Cisco Secure Email Gateway appliances. This will prevent messages from being stored in both quarantines and avoid confusion for end users and administrators.

質問: **17**
最近のスパム攻撃を受け、ネットワークエンジニアは組織のスパム対策ポリシーを強化する必要に迫られています。このような場合、どのシナリオにおいて、地域スキャンを有効にすることで組織のセキュリティが向上するのでしょうか？
A. 受信したメールのほとんどが米国外から送信されている場合
B. 受信したメールのほとんどが特定の地域から発信されている場合
C. 受信したスパムメールのほとんどが米国以外から発信されている場合
D. 受信したスパムメールのほとんどが特定の国から来ている場合
正解: (正解を表示します)
Enable or disable regional scanning and if applicable, select a region.
Enable this feature only if you receive the bulk of your email from the specified region. Because this feature optimizes the anti-spam engine for a particular region, it can reduce capture rates for other types of spam.
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_01100.html?bookSear ch=true

質問: **18**
Cisco ESAがCisco Registered Envelope Serviceを使用して電子メールを暗号化できるようにするには何を設定する必要がありますか？
A. プロビジョニングされたメール暗号化プロファイル
B. TLSで「メッセージの暗号化」を選択するコンテンツフィルターからのメッセージの暗号化
C. 「CRES」が選択されたメールフローポリシーからのメッセージ暗号化
D. 電子メールをCisco Registered Envelopeサーバーに転送するコンテンツフィルター
正解: (正解を表示します)
To allow the Cisco ESA to encrypt an email using the CRES (Cisco Registered Envelope Service), a provisioned email encryption profile must be configured on Cisco ESA. A provisioned email encryption profile is a type of encryption profile that specifies how messages are encrypted using CRES, such as the encryption key strength, the notification options, the branding settings, etc.
https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-cres-encryption.pdf

質問: **19**

企業のセキュリティポリシーでは、財務部門が機密データを含む送信メッセージに簡単に暗号化を適用できる方法を用意することが求められています。ユーザーは暗号化が必要なメッセージを識別できる必要があり、Cisco ESAがすべてのメッセージをスキャンして検出により自動的に暗号化するのではなく、ユーザーが暗号化が必要なメッセージにフラグを付ける必要があります。この機能を実現するには、どの操作を実行すればよいでしょうか？

A. 条件なしの送信コンテンツフィルタを作成し、件名設定で [SECURE] を設定した [暗号化して今すぐ配信] アクションを設定します。

B. 暗号化を有効にした DLP ポリシー マネージャー メッセージ アクションを作成し、送信メールのアクティブな DLP ポリシーに適用します。

C. 件名設定で[SECURE]を指定して暗号化プロファイルを作成し、メールフローポリシーで暗号化を有効にします。

D. 暗号化プロファイルと送信コンテンツフィルタを作成し、件名ヘッダー: 含む条件に \[SECURE\] を含め、暗号化して今すぐ配信するアクションを設定します。

正解: **D (**コメントを発表する**)**

To use encryption with the appliance , you must configure an encryption profile. After you create an encryption profile, you need to create an outgoing content filter that determines which email messages should be encrypted. The content filter scans outgoing email and determines if the message matches the conditions specified.

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_010010.html#con_1

171717

質問: **20**

組織は、既存のCisco ESAを使用して新しいドメインをホストし、そのドメインに個別の企業ポリシーを適用したいと考えています。

これを実現するには、Cisco ESAで何をする必要がありますか？

A. smtproutesコマンドを使用して、新しいドメインのSMTPルートを構成します。

B. deli very configコマンドを使用して、新しいドメインのメール配信を構成します。

C. dsestconfコマンドを使用して、新しいドメインに別の宛先を追加します。

D. altrchostコマンドを使用して、新しいドメイン用に別のゲートウェイを追加します。

正解: **(**正解を表示します**)**

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_011001.html

質問: **21**

管理者が、ウイルス対策ソフトのシグネチャが利用可能になる前に、マルウェアメールがESAを通過していることに気づいた。このような状況に対して最も効果的な保護を提供する機能はどれか？

A. グレイメール検出

B. SMTP認証

C. アウトブレイクフィルター

D. 受信者アクセステーブル

正解: **(**正解を表示します**)**

Outbreak Filters provide zero-hour protection by leveraging Cisco Talos intelligence, reputation data, and behavioral analysis. They can detect and quarantine suspicious messages during emerging malware campaigns before traditional anti-virus vendors release updated signatures.

質問: **22**

Cisco ESAに接続するために複数のLDAPサーバーで使用されている2つの構成はどれですか。 2つ選択してください。）

A. load balancing

B. SLA monitor

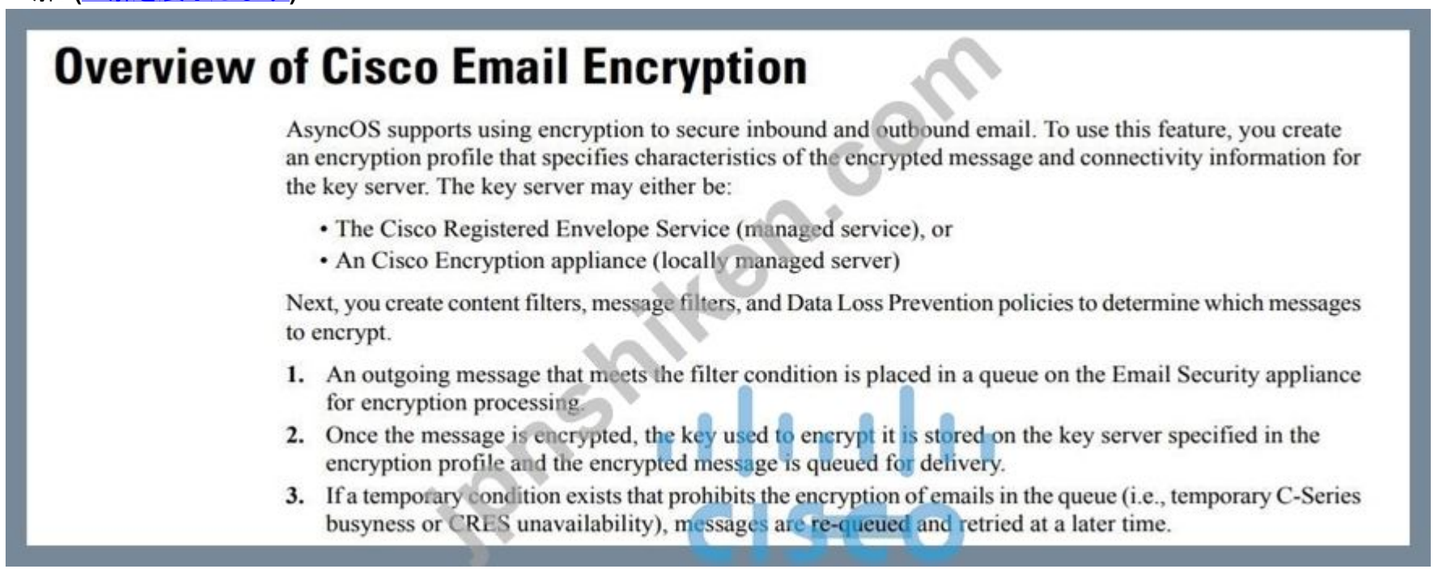
C. active-standby

D. failover

E. active-active

正解: (正解を表示します)
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

質問: **23**
電子メールの暗号化は、CRESを使用するCisco ESAで設定されます。
CRESが利用できない場合、メッセージに対してどのアクションが実行されますか？
A. キューに再登録されます。
B. クリアテキストで送信されます。
C. ドロップされ、エラーメッセージが送信者に送信されます。
D. Cisco暗号化アプライアンスによって暗号化されます。
正解: (正解を表示します)


Overview of Cisco Email Encryption

AsyncOS supports using encryption to secure inbound and outbound email. To use this feature, you create an encryption profile that specifies characteristics of the encrypted message and connectivity information for the key server. The key server may either be:

- The Cisco Registered Envelope Service (managed service), or
- An Cisco Encryption appliance (locally managed server)

Next, you create content filters, message filters, and Data Loss Prevention policies to determine which messages to encrypt.

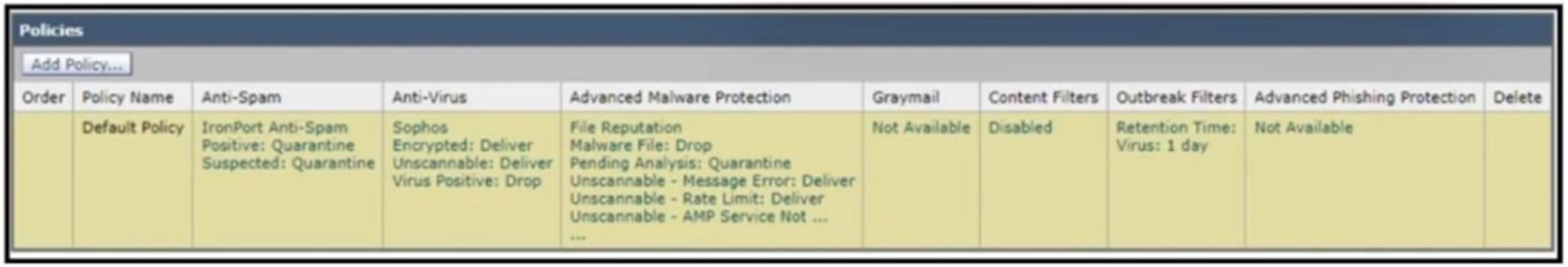
1. An outgoing message that meets the filter condition is placed in a queue on the Email Security appliance for encryption processing.
2. Once the message is encrypted, the key used to encrypt it is stored on the key server specified in the encryption profile and the encrypted message is queued for delivery.
3. If a temporary condition exists that prohibits the encryption of emails in the queue (i.e., temporary C-Series busyness or CRES unavailability), messages are re-queued and retried at a later time.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.577

質問: **24**
エンジニアは、Cisco Secure Email Gateway から Cisco SecureX へ脅威レポート情報を共有する必要があります。Secure Email Gateway で有効にする必要がある設定はどれですか？
A. SNMP
B. クラウドサービス設定
C. システムモニター
D. セキュリティサービス交換
正解: (正解を表示します)
To share threat reporting information from Cisco Secure Email Gateway to Cisco SecureX, the Security Services Exchange setting must be enabled. This integrates the email gateway with SecureX for unified threat visibility and reporting.

質問: **25**

図を参照してください。Cisco Secure Email Gatewayは、アウトブレイクフィルタによってスパムとアウトブレイクの両方に該当すると判定されたメールをどのように処理しますか？



A. メールはスパム隔離とアウトブレイク隔離に送られます。

B. メールは隔離措置のため送信され、公開前にスパムスキャンが再実施されます。

C. メールはスパム隔離フォルダにのみ送信されます。

D. メールは感染発生時の隔離措置にのみ送信されます。

正解: **C** (コメントを発表する)

When a message is identified as spam positive, the anti-spam action takes precedence and the message is placed only in the spam quarantine, even if outbreak filters also detect it as outbreak positive.

質問: **26**

セーフリストにあるsafedomain.comからメールを受信したときにスキップされるプロセスはどれですか。

A. メッセージフィルター

B. ウイルス対策スキャン

C. アウトブレイクフィルター

D. スパム対策スキャン

正解: (正解を表示します)

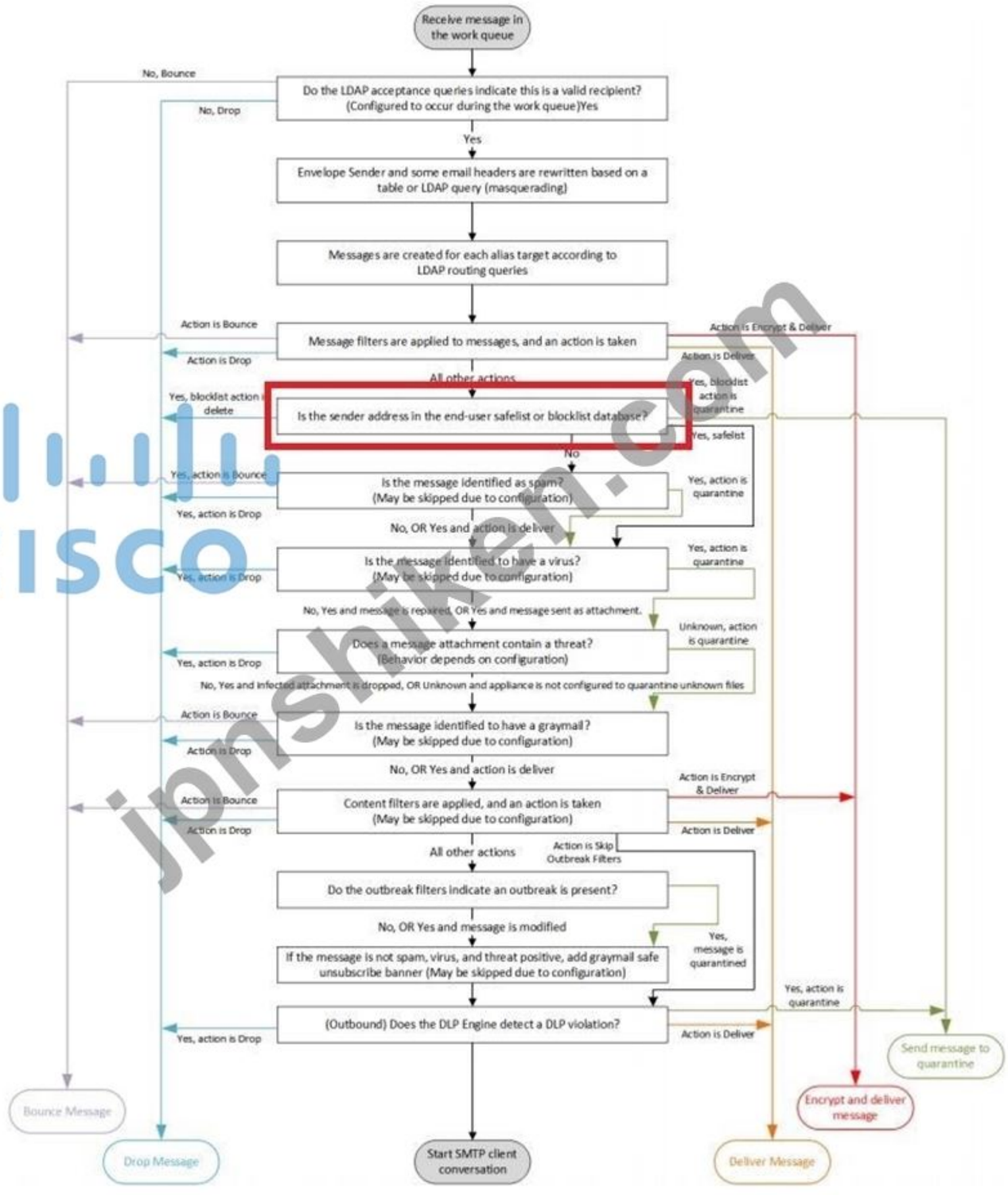
Message Processing of Safelists and Blocklists

A sender's being on a safelist or blocklist does not prevent the appliance from scanning a message for viruses or determining if the message meets the criteria for a content-related mail policy. Even if the sender of a message is on the recipient's safelist, the message may not be delivered to the end user depending on other scanning settings and results.

When you enable safelists and blocklists, the appliance scans the messages against the safelist/blocklist database immediately before anti-spam scanning. If the appliance detects a sender or domain that matches a safelist or blocklist entry, the message will be splintered if there are multiple recipients (and the recipients have different safelist/blocklist settings). For example, a message is sent to both recipient A and recipient B. Recipient A has safelisted the sender, whereas recipient B does not have an entry for the sender in the safelist or the blocklist. In this case, the message may be split into two messages with two message IDs. The message sent to recipient A is marked as safelisted with an *X-SLBL-Result-Safelist* header and skips anti-spam scanning, whereas the message bound for recipient B is scanned by the anti-spam scanning engine. Both messages then continue along the pipeline (through anti-virus scanning, content policies, and so on) and are subject to any configured settings.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.978

Figure 7: Email Pipeline — Work Queue



https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P. 123

質問: **27**
エンジニアは、Cisco Secure Email Gateway の altsrchost テーブルを変更する必要があります。@cisco.com というドメイン宛てのメッセージは、IP アドレスが 10.10.10.1 の NewInterface にマッピングする必要があります。
表には何を追加する必要がありますか？
A. NewInterface@cisco.com
B. cisco.com@ 10.10.10.1
C. @cisco.com NewInterface
D. cisco.com@ NewInterface
正解: **(**正解を表示します**)**
The altsrchost table maps a destination recipient domain to the source interface used for delivery.
Adding @cisco.com with NewInterface ensures messages destined for that domain are sent using the interface associated with IP address 10.10.10.1.

質問: **28**
ある組織は、メールに埋め込まれたURLに関して厳格なポリシーを設けています。このポリシーでは、URLの内容を確認することはできますが、ユーザーがクリックすることは許可されていません。セキュリティポリシーの要件を満たすには、どのような対策を講じる必要がありますか？
A. URLの牙を抜く。
B. URL隔離ポリシーを有効にする。
C. URLをテキストに置き換えます。
D. URLをCiscoセキュリティプロキシにリダイレクトします。
正解: **(**正解を表示します**)**
Defanging a URL means modifying it so that it is not clickable and cannot be directly accessed by a user, but still retains the visible structure of the original URL. This allows users to see the URL for informational purposes without being able to click on it and potentially open a malicious site.
Common defanging methods include replacing certain characters (like "." with "[dot]" or "http" with
"hxxp") to render the URL non-functional while keeping it recognizable.

質問: **29**
エンジニアは、社内ユーザーが受信するメールに含まれるURLによって、悪意のある外部コンテンツや望ましくない外部コンテンツへのアクセスによるデータ損失が発生しないようにしたいと考えています。この要件を満たすために、Cisco Secure Email Gatewayで設定する必要がある機能はどれですか？(2つ選択してください。)
A. スパム対策スキャン
B. データ損失防止
C. グレイメール検出
D. URLフィルタリング
E. ウイルス対策スキャン
正解: **(**正解を表示します**)**
To meet the requirement of ensuring that emails received by company users that contain URLs do not make them susceptible to data loss from accessing malicious or undesired external content sources, the administrator must configure two features on Cisco Secure Email Gateway:
antispam scanning and URL filtering. Antispam scanning can block or quarantine messages that are identified as spam based on various criteria, such as sender reputation, message content, and message headers. URL filtering can rewrite or defang URLs in messages that are associated with malicious or undesirable websites, such as phishing, malware, adult, or gambling sites.

質問: **30**
エンジニアは、Cisco Secure EmailをCisco Secure Endpointコンソールと統合する必要があります。ゼロデイ攻撃を防ぐために、どの2つの設定を構成する必要がありますか？(2つ選択してください。)
A. メッセージフィルター
B. ファイル評価フィルタリング
C. ファイル分析
D. 不適切なURL設定
E. コンテンツフィルタ設定
正解: **(**正解を表示します**)**
To integrate Cisco Secure Email with Cisco Secure Endpoint and block zero-day threats, the engineer must enable File Reputation Filtering (to check files against Cisco's threat intelligence) and File Analysis (to send unknown or suspicious files to Threat Grid for sandboxing and behavioral analysis). These two settings work together to detect and block zero-day malware.

質問: **31**
Cisco ESA管理者は、ユーザが特定のドメインから電子メールを受信していないことを通知されました。メールログを確認した後、送信者は送信者ベースのレピュテーションスコアが負でした。
その特定のドメインからの受信メールを許可するには、管理者は何をする必要がありますか？
A. ドメインを許可リストに追加します。
B. ドメインからのメールを許可するようにファイアウォールを変更します。
C. Talosをオーバーライドするメッセージフィルターを使用して、新しい受信メールポリシーを作成します。
D. メールアプリケーションの許可リストに送信者を追加するようにユーザーに依頼します。
正解: **(**正解を表示します**)**

質問: **32**
Cisco SMAで外部スパム検疫を有効にするとどのようなメリットがありますか？
A. 複数のCisco ESAから1つの中央コンソールにスパム検疫をバックアップする機能
B. ユーザーが解放、複製、または削除できるスパム検疫インターフェースへのアクセス
C. 2つのエンジンを使用してメッセージをスキャンし、キャッチ率を上げる機能
D. スパム検疫データを複数のCisco ESAから1つの中央コンソールに統合する機能
正解: **(**正解を表示します**)**
The Security Management appliance includes the following features:
External spam quarantine. Holds spam and suspected spam messages for end users, and allow end users and administrators to review messages that are flagged as spam before making a final determination.
Centralized policy, virus, and outbreak quarantines. Provide a single location behind the firewall to store and manage messages quarantined by anti-virus scanning, outbreak filters, and policies.
Centralized reporting. Run reports on aggregated data from multiple Email Security appliances.
Centralized tracking. Track email messages that traverse multiple Email Security appliances.

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_0101010.html?bookSe arch=true

質問: **33**
エンジニアがフラグ付きメッセージを特定の仮想ゲートウェイアドレスに最も柔軟な方法で配信できるようにする方法はどれですか。
A. フラグでインターフェースグループを設定します。
B. altsrchostコマンドを発行します。
C. エンベロープ送信者アドレスをホストにマップします。
D. メッセージにフィルターを適用します。
正解: **(**正解を表示します**)**
Users requiring more power and flexibility in mapping messages to particular Virtual Gateways should investigate the use of message filters.
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_011001.html

質問: **34**
ある組織は、メッセージ送信開始前に、評判の非常に悪いホストからのSMTP接続をESAが拒否するようにしたいと考えています。最初に設定すべき機能はどれでしょうか？
A. コンテンツフィルター
B. 受信メールポリシー
C. SBRSしきい値を含むホストアクセステーブル(HAT)
D. アウトブレイクフィルター
正解: **(**正解を表示します**)**
HAT evaluates the sender IP during SMTP connection establishment and can use SenderBase Reputation Score (SBRS) values to accept, throttle, or reject connections before message data is transmitted. This conserves system resources and blocks unwanted traffic at the earliest possible stage.

質問: **35**
Cisco Secure Email Gateway のスパム隔離機能にエンドユーザーがアクセスできるようにする認証設定はどれですか？(2つ選択してください。)
A. チャップ
B. 郵便受け
C. LDAP
D. 半径
E. TACACS+
正解: **(**正解を表示します**)**
End-user access to the spam quarantine can be authenticated using mailbox authentication or LDAP authentication. These methods allow users to log in and manage quarantined spam messages associated with their email accounts.

質問: **36**
送信者のドメインやその他の属性に基づいて電子メール メッセージのレピュテーション判定を提供するクラウド サービスはどれですか?
A. Cisco AppDynamics
B. Cisco Secure Email Threat Defense
C. シスコ セキュア クラウド分析
D. Cisco Talos
正解: **D (**コメントを発表する**)**

Cisco Talos is a cloud service that provides a reputation verdict for email messages based on the sender domain and other attributes such as IP address, sender behavior, message content, and attachment analysis. Cisco Talos is integrated with Cisco Secure Email Gateway and provides real-time threat intelligence and protection against spam, phishing, malware, and other email- borne threats.

質問: **37**
Cisco ESAにURLフィルタリングを実装する利点は何ですか？
A. 悪意のあるURLから脅威を削除します
B. スパムをブラックリストに登録
C. URLレピュテーション保護を提供します
D. 悪意のあるURLに対する評判を高める
正解: **C (**コメントを発表する**)**
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html

質問: **38**
コンテンツフィルターの機能とは何ですか？
A. メールの件名に基づいてメッセージをレビューする
B. スパム対策スキャンを実行する
C. 受信または送信メッセージをスキャンする
D. メッセージフィルターの前にルールを適用する
正解: **(**正解を表示します**)**
Content filters can scan both incoming and outgoing messages for specific criteria such as keywords, attachments, or other attributes to enforce organizational policies.

質問: **39**
使用されているカスタム検疫を削除する前に、どのアクションを実行する必要がありますか？
A. フィルターに割り当てられている隔離を削除します。
B. フィルターに割り当てられていない隔離を削除します。
C. 未使用の検疫のみを削除します。
D. フィルターのメッセージアクションから隔離を削除します。
正解: **(**正解を表示します**)**
Before a custom quarantine that is being used can be deleted, it must be removed from the message action of any filter that is using it on Cisco ESA. Otherwise, an error message will appear stating that the quarantine cannot be deleted because it is in use.
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

質問: **40**
SDR名がPOORの場合、推奨される対処法は何ですか？
A. メッセージを許可します。
B. 他のエンジンでメッセージをスキャンします。
C. メッセージを隔離します。
D. メッセージをブロックします。
正解: **D (**コメントを発表する**)**
An SDR rating of Poor indicates a highly negative sender reputation, so the recommended action is to reject or block the message before further processing.

質問: **41**
バウンス検証は、どのような種類の攻撃に対抗するのでしょうか？
A. スピアフィッシング
B. 後方散乱
C. フィッシング
D. アイデンティティ
正解: **(**正解を表示します**)**
Bounce Verification is designed to fight against backscatter attacks, where a mail server receives nondelivery reports for emails that were spoofed with the victim's address as the sender. Bounce Verification ensures that only legitimate bounce messages are accepted.

質問: **42**
エンジニアは、組織内の役員向けに差別化されたメールフィルタリングを提供する必要があります。このタスクを達成するために、どの2つのアクションを実行する必要がありますか？(2つ選択してください)
A. メールポリシー規則が適用されるユーザーを指定するために、LDAPグループクエリを定義します。
B. 特定のデータを含むメッセージに対して実行するアクションのコンテンツフィルタを作成します。
C. メールポリシーを作成するユーザーのメールアドレスを含むCSVファイルをアップロードしてください。
D. メールポリシーで使用するコンテンツスキャン機能を有効にします
E. 受信または送信メッセージのデフォルトメールポリシーを定義します
正解: **(**正解を表示します**)**
Define an LDAP group query to specify users to whom the mail policy rules apply. This way, you can create a custom group of executive users and apply different mail policies to them based on their LDAP attributes.
Create content filters for actions to take on messages that contain specific data. Content filters allow you to scan the message body and attachments for keywords, phrases, or patterns that match your criteria and perform actions such as quarantine, encrypt, or drop the message.

質問: **43**
偽造メール検出に使用するコンテンツ辞書が作成されました。CEO Example CEO」に関する適切なデータを入力する必要があります。この目的を達成するには、辞書に何を追加する必要がありますか？
A. CEO
B. CEOの例
C. ceo@example.com
D. example.com
正解: **B (**コメントを発表する**)**
Setting Up Forged Email Detection
Identify the users in your organization (for example, executives) whose messages are likely to be forged. Create a new content dictionary and add the names of the identified users to it.
While creating a content dictionary,
Enter the name of the user and not the email address. For example, enter "Olivia Smith" instead of "olivia.smith@example.com."
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#co n_1260492

質問: **44**

ある組織が外部の企業との間でTLS接続を強制しています。外部企業は独自の内部認証局(CA)を使用しているため、セキュアメールゲートウェイはTLS接続を検証できません。Ciscoセキュアメールゲートウェイが接続を信頼するために、エンジニアはどのような対策を講じる必要がありますか？
A. 宛先制御を変更し、すべての外部および内部宛先に対してTLSサポートを必須に設定します。
B. ネットワーク > 証明書ページでカスタムリストを有効にし、信頼できる認証局の証明書をアップロードします。
C. 宛先コントロールを編集し、外部パーティドメインを信頼済みとして宛先コントロールテーブルに追加します。
D. [ネットワーク] > [証明書] ページで [証明書の追加] を選択し、自己署名証明書を作成します。
正解: **(**正解を表示します**)**
To trust the TLS connection with an external party using its own internal CA, the engineer must enable a custom list on the Network > Certificates page and upload the external CA's certificates.
This allows the Cisco Secure Email Gateway to validate and trust certificates signed by that internal CA.

質問: **45**
エンジニアは、標準の H 機能のみが動作しないことを許可するデフォルト設定で Cisco Secure Email Gateway アプライアンスを組織に導入します。問題を解決するには、どのような追加アクションを実行すればよいですか?
A. ポート 8081 でのトラフィックを許可するように送信ファイアウォール ルールを構成します。
B. ファイル レピュテーションの詳細設定で [HTTP を使用] オプションを有効にします。
C. ファイル レピュテーションの詳細設定で SSL を使用するオプションを有効にします。
D. ポート 3237 でのトラフィックを許可するように送信ファイアウォール ルールを構成します。
E. TP/HTTPS ポートが送信され、AMP ファイルのレピュテーションが通知されます。
正解: **E (**コメントを発表する**)**
Configuring the outbound firewall rule to permit traffic on port 3237 is the additional action that resolves the issue. AMP file reputation is a feature that allows Cisco ESA to check files attached to messages against a cloud-based database of known malicious files and apply appropriate actions, such as block, deliver, or quarantine.
By default, AMP file reputation uses TCP port 3237 to communicate with the cloud-based database. If this port is blocked by a firewall, AMP file reputation will not work properly. To resolve this issue, the administrator can configure the outbound firewall rule to permit traffic on port 3237 from Cisco ESA.

質問: **46**
Cisco ESAのグレイメール管理ソリューションを構成する2つのコンポーネントはどれですか。 2つ選択してください。）
A. クラウドベースの退会サービス
B. エンドユーザー向けの統一サブスクリプション管理インターフェイス
C. エンドユーザー向けの安全なサブスクライブオプション
D. 統合されたグレイメールスキャンエンジン
E. メールの有効性の向上
正解: **(**正解を表示します**)**
The graymail management solution in the appliance comprises of two components: an integrated graymail scanning engine and a cloud-based Unsubscribe Service. The integrated graymail scanning engine identifies graymail messages using various criteria and assigns them to different categories. The cloud-based Unsubscribe Service provides an easy mechanism for end users to unsubscribe from unwanted messages by checking the reputation of the unsubscribe links and performing the unsubscribe process on behalf of the end user.
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)

質問: **47**
エンジニアは、DMARCを使用してCisco Secure Email Gatewayで受信メッセージの検証を設定する必要があります。admin@cisco.comからのメールは検証をスキップする必要があります。以下の設定は既に完了しています。
- DMARC検証プロファイルを作成します。
- グローバル DMARC 設定を構成して検証をスキップします
admin@cisco.com
タスクを完了するために実行しなければならない2つの行動はどれですか？(2つ選択してください。)
A. DMARCポリシー用のLDAPサーバープロファイルを設定します。
B. DMARC検証ポリシーを作成します。
C. メールフローポリシーでDMARC検証を有効にする。
D. メールフロープロファイルにDMARC検証を実装します。
E. 送信者バイパスアドレスリストを設定します。
正解: **B,C (**コメントを発表する**)**
DMARC verification requires a DMARC verification policy that defines how incoming messages are evaluated and handled. DMARC verification must then be enabled on the applicable mail flow policy so the Cisco Secure Email Gateway applies the verification profile and policy to inbound SMTP traffic.

質問: **48**
メッセージフィルター処理を構成するときに考慮する必要がある2つの要素はどれですか。 2つ選択してください。）
A. メッセージフィルターの順序
B. ラテラル加工
C. 結合されたパケットの構造
D. メールポリシー
E. メッセージのMIME構造
正解: **A,E (**コメントを発表する**)**
Message-filter order and MIME structure of the message are two factors that must be considered when message filter processing is configured on Cisco ESA. Message-filter order determines the sequence in which message filters are evaluated and applied to incoming messages, which can affect the final outcome of the filtering process. MIME structure of the message determines how message filters match against different parts of the message, such as headers, body, attachments, etc., which can affect the accuracy and performance of the filtering process.
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

質問: **49**
ドラッグアンドドロップ問題
エンジニアは、Cisco Secure Email Gatewayで暗号化を有効にする必要があります。各メッセージの最大サイズは20MBです。要件を満たすように、左側のアクションを右側にドラッグアンドドロップして順番に並べ替えてください。

Answer Area

正解:

Answer Area

Explanation:
This order ensures encryption is enabled before editing settings to apply the message size limit.

質問: **50**
セキュリティ管理者は、Cisco Secure Email Gateway 上でアウトブレイクフィルタに関するアラートを設定したいと考えています。
要件を満たすために取るべき2つの行動はどれですか？(2つ選択してください。)
A. 適応ルールを使用して、アウトブレイクフィルターのアラートを有効にします。
B. システム管理からメッセージ分割を有効にします。
C. セキュリティサービスから、アウトブレイクフィルタの設定を構成します。
D. アウトブレイクフィルターのグローバル設定から、アウトブレイクフィルターのアラートを有効にします。
E. メールポリシーから、アウトブレイクフィルタの設定を構成します。
正解: **C,D (コメントを発表する)**
Outbreak Filters must first be configured under Security Services so the appliance can apply outbreak filtering. Alerts are then enabled in the Outbreak Filters Global Settings, which controls alert generation for outbreak filter events.

質問: **51**
グレーメールを分類するためのカテゴリとは何ですか？
A. 優先
B. マーケティング
C. 悪意のある
D. スパム
正解: **(**正解を表示します**)**
Graymail Classification
The graymail engine classifies each graymail into one of the following categories:
* Marketing Email. Advertising messages sent by professional marketing groups, for example, bulletins from Amazon.com with details about their newly launched products.
* Social Network Email. Notification messages from social networks, dating websites, forums, and so on. Examples include alerts from:
* LinkedIn, for jobs that you may be interested in
* CNET forums, when a user responds to your post.
* Bulk Email. Advertising messages sent by unrecognized marketing groups, for example, newsletters from TechTarget, a technology media company.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide/b_ESA_Admin_Guide/b_ESA_Admin_Guide_chapter_01101.pdf

質問: **52**
エンジニアが新しいCiscoESAでメールフローをテストしていて、ドメインabc.comのメッセージが配信キューでスタックしていることに気付きました。さらに調査すると、エンジニアは、配信待ちのメッセージが192.168.1.11宛てであることに気付きましたが、代わりに192.168.1.10にルーティングする必要があります。
この問題に対処するには、どのような構成変更が必要ですか？
A. ドメインabc.comのアドレスリストを追加します。
B. ドメインabc.comのDestinationControlsエントリを変更します。
C. ドメインのSMTPルートを変更し、IPアドレスを192.168.1.10に変更します。
D. ルーティングテーブルを変更し、IPアドレスのルートを192.168.1.10に追加します。
正解: **(**正解を表示します**)**
SMTP Routes allow you to redirect all email for a particular domain to a different mail exchange (MX) host.
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_011001.html?bookSea rch=true

質問: **53**
Cisco ESAが集中型メッセージ追跡を使用するように構成されている場合、デバイスとCisco Security Management Appliance間のデフォルトポートはどれですか？
A. ポート22/TCP
B. ポート53/UDP
C. ポート80/UDP
D. ポート25/UDP
E. ポート23/TCP
正解: **A (**コメントを発表する**)**

質問: **54**
図を参照してください。ネットワークエンジニアは、SPF認証に失敗したメッセージを検出して隔離するために、コンテンツフィルタを設定する必要があります。コンテンツフィルタは設定され、有効化されていますが、SPF認証に失敗したメッセージ以外のすべてのメッセージが隔離されています。この動作を修正するには、フィルタのどの部分を変更する必要がありますか？

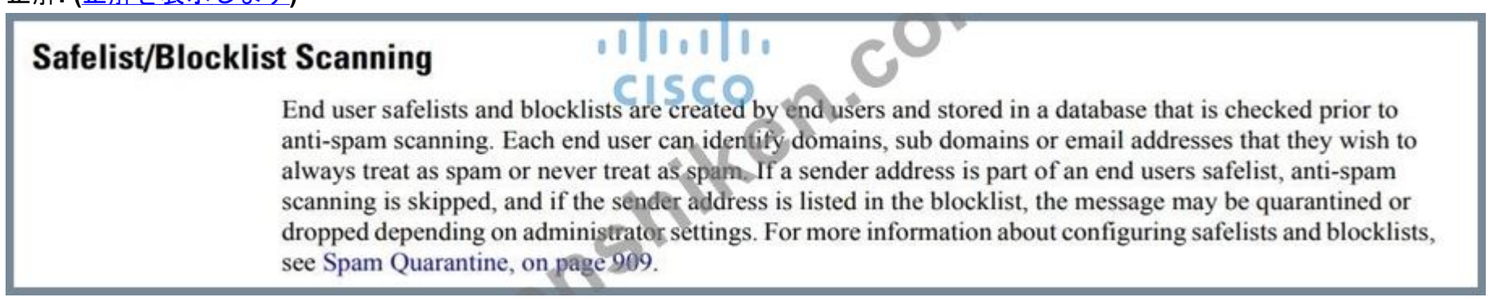

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	SPF-QUARANTINE-FAIL	SPF-QUARANTINE-FAIL: if(spf-status != "fail") {log-entry("*** SPF FAILED QUARANTINE ***"); quarantine("Policy"); skip-filters(); }		

A. ログエントリ
B. 検疫
C. SPFステータス
D. フィルターをスキップ
正解: **C (**コメントを発表する**)**
You can check against the SPF/SIDF verification results using the following syntax:
if (spf-status == "Pass")
If you want a single condition to check against multiple status verdicts, you can use the following syntax:
if (spf-status == "PermError, TempError")
You can also check the verification results against the HELO, MAIL FROM, and PRA identities using the following syntax:
if (spf-status("pra") == "Fail")
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_01000.html?bookSearch=true#con_1132105

質問: **55**
スパムである電子メールを受信トレイに配信して、Cisco ESAでのスパム判定およびアクションを上書きできるようにエンドユーザーが制御できるようにするために、どのアンチスパム機能が利用されていますか？
A. エンドユーザー許可リスト
B. エンドユーザーのスパム検疫アクセス
C. エンドユーザーパススルーリスト
D. エンドユーザーセーフリスト
正解: (正解を表示します)


Safelist/Blocklist Scanning

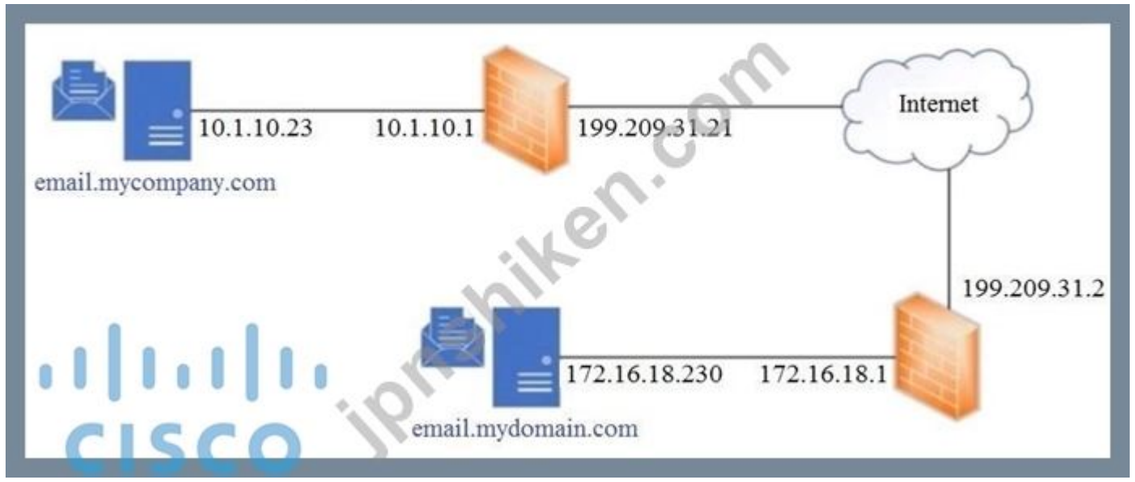
End user safelists and blocklists are created by end users and stored in a database that is checked prior to anti-spam scanning. Each end user can identify domains, sub domains or email addresses that they wish to always treat as spam or never treat as spam. If a sender address is part of an end users safelist, anti-spam scanning is skipped, and if the sender address is listed in the blocklist, the message may be quarantined or dropped depending on administrator settings. For more information about configuring safelists and blocklists, see Spam Quarantine, on page 909.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.129

質問: **56**
最近の監査に対応するため、エンジニアは受信メールポリシーでウイルス対策メッセージ処理オプションを設定し、メールの件名に警告を添付するようにする必要があります。
既知のウイルスメールに関するこの要件を満たすには、どのような設定が必要でしょうか？
A. ウイルス感染メッセージ
B. スキャンできないメッセージ
C. 暗号化されたメッセージ

D. 肯定的に識別されたメッセージ
正解: **(**正解を表示します**)**
To meet the requirement of attaching warnings to the subject of an email for known viral emails, the appropriate option to configure would be for handling virus-infected messages. Known viral emails are those that are positively identified as containing a virus by the anti-virus scanning mechanism.
This setting specifically deals with emails that have been identified as containing a virus, and configuring this will allow the engineer to attach warnings to the subject line of such emails, thereby complying with the audit requirement.

質問: **57**
グレイメールセーフ購読解除機能はどのように機能しますか
A. 登録解除する前に、URIの悪意のあるコンテンツを取り除きます。
B. URIレピュテーションとカテゴリーをチェックし、コンテンツフィルターがアクションを実行できるようにします。
C. 登録解除ボタンをクリックしたエンドユーザーをサンドボックス環境にリダイレクトして、安全な登録解除を許可します。
D. URIの評判をチェックし、エンドユーザーに代わって登録解除プロセスを実行します。
正解: **D (**コメントを発表する**)**
Secure unsubscribe option for end users. Mimicking an unsubscribe option is a popular phishing technique. For this reason, the end users are generally wary of clicking unknown unsubscribe links. For such scenarios, the cloud-based Unsubscribe Service extracts the original unsubscribe URI, checks the reputation of the URI, and then performs the unsubscribe process on behalf of the end user. This protects end users from malicious threats masquerading as unsubscribe links.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200383-Graymail-Detection-and-Safe-Unsubscribin.html

質問: **58**
図を参照してください。mycompany.comに対して有効なSPFレコードはどれですか？


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
正解: **(**正解を表示します**)**
The SPF record for mycompany.com is shown in the exhibit as:
v=spf1 a mx ip4:199.209.31.21 -all

This means that the domain mycompany.com authorizes the following sources to send email on its behalf:
The A record of mycompany.com, which resolves to 199.209.31.21
The MX record of mycompany.com, which points to mail.mycompany.com, which also resolves to 199.209.31.21
The IP address 199.209.31.21
The -all qualifier means that any other source is not authorized and should be rejected.

質問: **59**
Cisco Email Security Applianceは、どのようなサービス上の問題を2つ解決できますか？(2つ選択してください。)
A. IPS
B. DLP
C. スパム対策
D. URLフィルタリング
正解: **(正解を表示します)**

質問: **60**
Cisco ESA は、評判スコアが -6 を超えるメールはログに記録され、-6 未満のメールはログに記録され、暗号化されてから配信されるように構成されています。メール本文に、ネストされた短縮 URL の制限を超える短縮 URL が含まれています。このメールに対してどのようなアクションが実行されますか？
A. 暗号化されていますが、ログには記録されません。
B. ログには記録されますが、暗号化はされません。
C. ログに記録され、破棄されます。
D. ログが記録され、暗号化されます。
正解: **(正解を表示します)**
The shortened URL can be redirected to a maximum limit of 10 nested shortened URLs to determine the actual URL.
If the shortened URL exceeds the maximum limit of 10 nested shortened URLs, a URL reputation score of -10 is assigned to the shortened URL by default.
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_01111.html

質問: **61**
セキュリティ管理者は、レビューのために疑わしいスパムを保存するように設定されたメール ポリシーを備えた Cisco Secure Email Gateway アプライアンスを導入しました。アプライアンスは DMZ であり、標準の HTTP/HTTPS ポートのみがファイアウォールによって許可されます。管理者は、ブロックされたスパムの疑いがあるものをユーザーが確実に表示できるようにしたいと考えています。この要件を満たすためにはどのような措置を講じる必要がありますか?
A. 外部スパム隔離を有効にし、Secure Email and Web Manager の IP アドレスとポートを入力します。
B. スパム隔離を有効にし、デフォルト設定を変更しないままにします。
C. エンドユーザー隔離アクセスを有効にし、認証用に LDAP サーバーを指定します。
D. スパム隔離を有効にし、HTTP にはポート 80、HTTPS にはポート 443 を指定します。
正解: **(正解を表示します)**
Enabling End-User Quarantine Access and pointing to an LDAP server for authentication is the action that must be taken to meet this requirement. End-User Quarantine Access is a feature that allows users to access their personal quarantine on Cisco ESA using their email address and password, without requiring an administrator account or access to Secure Email and Web Manager. To enable End-User Quarantine Access on Cisco ESA, the administrator can follow these steps:
Select Security Services > IronPort Anti-Spam > End User Safelist/Blocklist Settings and click Edit Settings.

Under End User Quarantine Access, select Enable End User Quarantine Access. Under Authentication Server, select LDAP Server from the drop-down menu and choose an LDAP server profile from the drop-down menu.
Click Submit.

質問: **62**
添付資料を参照してください。隔離エリアにアクセスする前にエンドユーザー認証を強制するために、どのような措置を講じる必要がありますか？

A. スパム通知を有効にし、認証にLDAPを使用します。
B. スパム隔離通知を有効にし、%quarantine_url% 変数を追加します。
C. エンドユーザーの隔離アクセスを認証なしからSAASに変更します。
D. エンドユーザーの隔離アクセス設定を認証なしからメールボックスに変更します。
正解: **(**正解を表示します**)**
In the Spam Notifications settings, deselect or select Enable login without credentials for quarantine access.
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_0100000.html

質問: **63**
ネットワーク エンジニアがメール フローの問題のトラブルシューティングを行っているとき、一部の電子メールが SMTP コード 451 とエラー メッセージ #4.7.1 DMARC 検証を実行できません」で拒否されていることを発見しました。Cisco Secure Email Gateway アプライアンスの DMARC 検証プロファイルでは、一時的な失敗を引き起こすメッセージに対して、これらの電子メールが拒否されないようにするにはどのアクションを設定する必要がありますか?
A. 受け入れる
B. 無視する
C. 隔離
D. アクションなし
正解: **A (**コメントを発表する**)**
To prevent emails from being rejected due to temporary DMARC verification failures (SMTP code
451), the DMARC verification profile action must be set to Accept. This allows messages with temporary verification issues to be delivered instead of rejected.

質問: **64**
図を参照してください。フィルター2をアクティブに設定するための正しいコマンドの順序は何ですか？

Num	Active	Valid	Name
1	Y	Y	Anti_Spoofing
2	N	Y	Skip-filter
3	Y	Y	WHITELIST

A. フィルター→編集→2→アクティブ
B. フィルター→変更→すべて→有効
C. フィルター→詳細→2→1
D. フィルター→設定→2→1
正解: **D** (コメントを発表する)
Message Filters Subcommands.
set: Sets filter to active or inactive state. For more information, see Creating a New Message Filter.
For Example, using the filter -> set subcommand.
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?bookSear ch=true

質問: **65**
ネットワークエンジニアが、Cisco ESA 上でアウトブレイクフィルタ機能を使用してウイルスアウトブレイクフィルタを実装し、コンテンツフィルタを使用して追加のスキャンを実行する予定です。アウトブレイクフィルタはどのようなアクションを実行する必要がありますか？
A. 2つのエンジンを同時に使用して、処理済みのメッセージをスキャンします。
B. メッセージのコピーを隔離先に送信する。
C. 処理済みのメッセージをCisco ESAに送信します。
D. Cisco ESA のセカンダリ インスタンスを使用して、処理済みメッセージをスキャンします。
正解: **C** (コメントを発表する)
If you want to perform a content filter-based scan on the Outbreak Filter processed messages, you must configure the Outbreak Filter to send the processed messages back to an appliance.
This is because, in the processing pipeline, the Outbreak Filter scan is performed after the content filter scan.
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_01110.html?bookSear ch=true#con_1138405

質問: **66**
ある組織は、特許に関する機密文書が電子メールを介して外部に共有されることを防ぎたいと考えています。ネットワーク管理者はCisco ESA上のDLPポリシーを確認しましたが、適切な一致パターンを持つ既存のポリシーが見つかりませんでした。この要件を満たすポリシーを作成するには、どのタイプのDLPポリシーテンプレートを使用する必要がありますか？
A. 規制遵守
B. 許容される使用
C. カスタムポリシー
D. プライバシー保護
正解: (正解を表示します)
To create a DLP policy that specifically targets preventing the sharing of proprietary patent documents via email, the network administrator should use a custom policy template. A custom policy allows for the creation of tailored DLP rules and matching patterns based on the organization's specific requirements and data protection needs.
While regulatory compliance, acceptable use, and privacy protection policy templates may provide some predefined rules and patterns, they may not directly address the specific requirement of preventing the external sharing of proprietary patent documents. Therefore, a custom policy template would be the most suitable option as it provides flexibility in designing and implementing DLP rules specifically for the organization's unique data protection objectives.

質問: **67**
外部の検疫を有効にする前に、ローカルのスパム検疫を無効にするために必要な2つの手順はどれですか。 2つ選択してください。）
A. [スパム検疫を有効にする]チェックボックスをオフにします。
B. [監視]を選択し、[スパム検疫]をクリックします。
C. [外部セーフリスト/ブロックリスト]チェックボックスをオンにします。
D. [外部スパム検疫]を選択し、[構成]をクリックします。
E. [セキュリティサービス]を選択し、[スパム検疫]をクリックします。
正解: **(**正解を表示します**)**
Configuration Summary:
1) Enable centralized quarantine on the ESA appliance(s):GUI > Security Services > Spam Quarantine >Check Enable External Spam Quarantine
2) Disable the local quarantine(s):GUI > Monitor > Spam Quarantine> Uncheck Enable Spam Quarantine
3) Submit and Commit Changes.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa-00.html

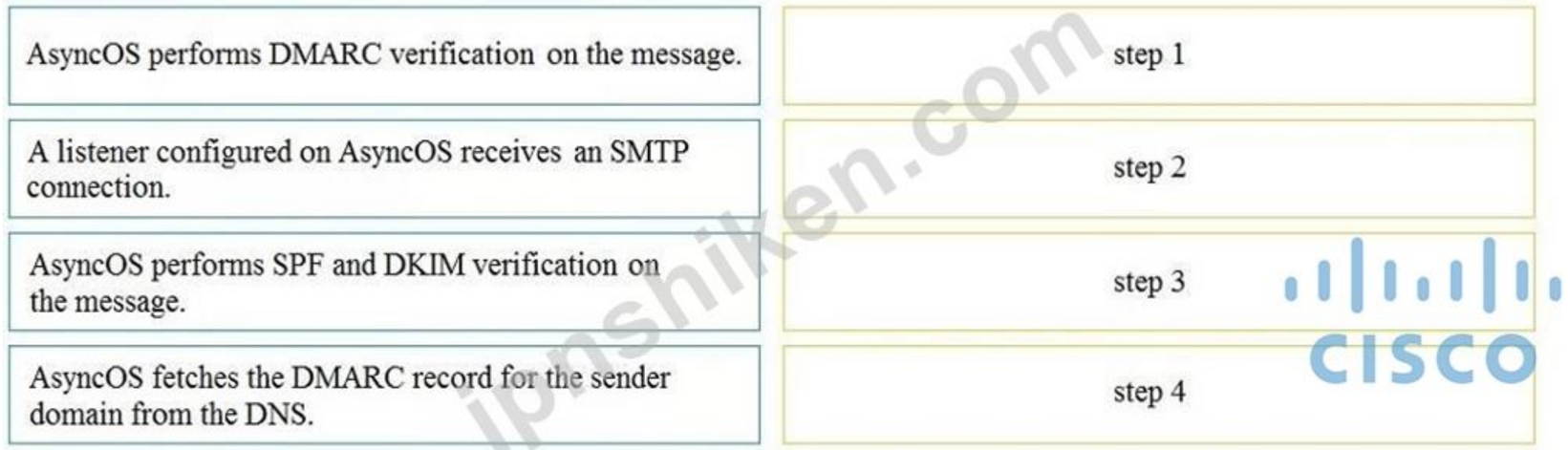
質問: **68**
グレイメールサービスの利点は何ですか？
A. クラウドおよびオンサイトでの解約サービスを提供
B. ソーシャルネットワークのメールマガジンに安全に登録できる方法を提供します
C. 不要なマーケティングメールの購読を解除するオプションを提供します。
D. 送信者のメールアドレスに基づいてスパムを削除します
正解: **(**正解を表示します**)**
Graymail services provide users with the option to unsubscribe from unwanted marketing emails, reducing inbox clutter from legitimate but unwanted mass mailings.

質問: **69**
Active Directoryサーバーへの LDAP認証を使用する場合、スパム隔離エンドユーザー認証クエリで使用されるデフォルトのプライマリメール属性は何ですか？
A. ユーザーアカウント
B. mailLocalAddress
C. sAMAccountName
D. プロキシアドレス
正解: **D (**コメントを発表する**)**
By default, the primary email attribute is proxyAddresses for Active Directory servers and mail for OpenLDAP servers. You can enter your own query and email attributes. To create the query from the CLI, use the isqauth subcommand of the ldapconfig command.
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

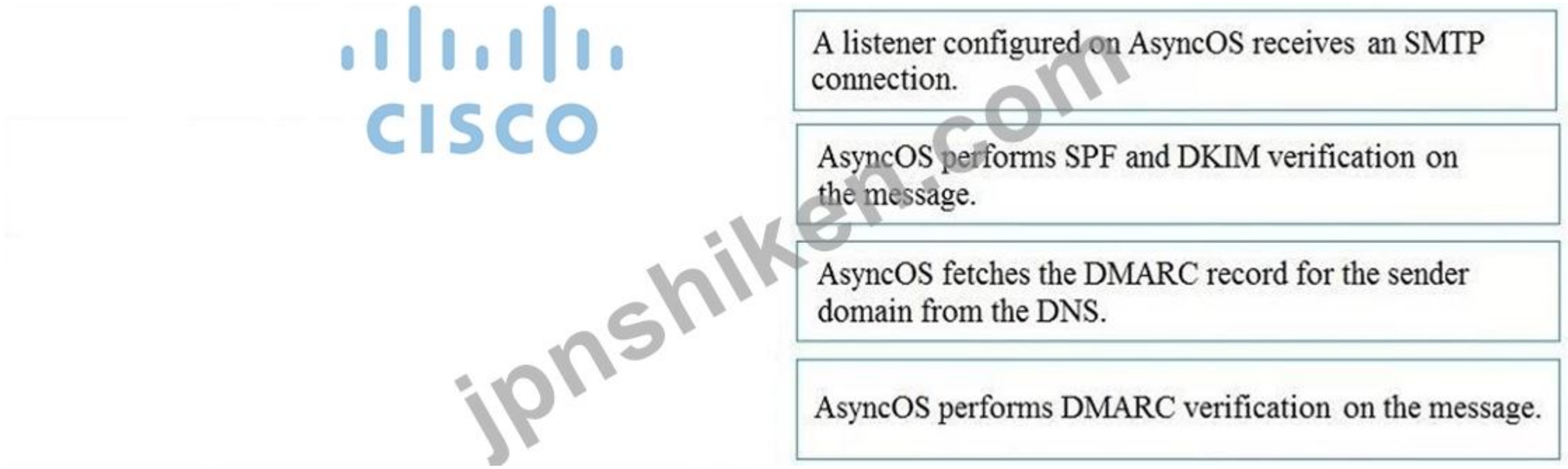
質問: **70**
エンドユーザー隔離へのログイン時に、LDAPを介してユーザーを認証する仕組みは何ですか？
A. エンドユーザー認証クエリ
B. 外部認証クエリ
C. エイリアス統合クエリ

D. LDAP認証クエリ
正解: (正解を表示します)
LDAP authentication query is used to validate users during login to end-user quarantine, ensuring that only authorized users can access their quarantined messages.

質問: **71**
ドラッグアンドドロップ問題
DMARC検証を実行するためのAsyncOSメソッドを、左側から右側の正しい順序にドラッグアンドドロップしてください。



正解:



質問: **72**
ネットワーク管理者は、組織のドメイン保護を有効にするために送信メールポリシーを変更しています。公開鍵を持つDNSエントリが作成されます。
送信メールポリシーの一致基準として使用される2つのヘッダーはどれですか？ (2つ選択してください。)
A. メッセージID
B. 送信者

C. URLレピュテーション
D. から
E. メール差出人
正解: **(**正解を表示します**)**
DomainKeys and DKIM Authentication
With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography. The verified domain can then be used to detect forgeries by comparing it with the domain in the From: (or Sender:) header of the email.
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_010101.html?bookSea rch=true

質問: **73**
エンジニアは初めてCiscoESAを設定し、内部SMTPサーバからの電子メールトラフィックがCisco ESAを介して中継され、送信メールポリシーに関連付けられていることを確認する必要があります。
この目標を達成するには、どのメールフローポリシー設定を変更する必要がありますか？
A. 例外リスト
B. 接続動作
C. バウンス検出署名
D. 逆接続検証
正解: **B (**コメントを発表する**)**
Mail Flow Policies
These are the policies that apply to the Sender Groups of the ESA, on the basis of which email traffic modulation is done.
Mail Flow Policies always applies to traffic which is Incoming to the ESA irrespective of the email being an Inbound or Outbound one.
The Mail Flow Policies works in the backend with regards to the selected Connection Behavior for that policy. The different Connection Behavior available in ESAs are:
- Accept
- Reject
- Relay
- TCP Refuse
- Continue
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216842-understand-parameters-related-to-mail-fl.html

質問: **74**
ネットワークエンジニアがCisco Secure Email GatewayとCisco SecureXを統合している。
Cisco Secure Email GatewayをCisco SecureXに登録する前に、必ず実行しなければならない2つの手順はどれですか？(2つ選択してください。)
A. Securexでthreatresponseconfigコマンドを実行します。
B. ファイアウォールでTCPポート22を開放します。
C. SecureXでcloudserviceconfigコマンドを実行します。
D. SecureXで管理者アカウントを作成します。
E. ファイアウォールでTCPポート443を開放してください。
正解: **(**正解を表示します**)**
Cisco Secure Email Gateway must have cloud service connectivity enabled before SecureX registration, and outbound HTTPS access over TCP port 443 is required so the gateway can communicate with Cisco cloud services.

質問: **75**
仮想ゲートウェイが構成されている場合、各仮想ゲートウェイアドレスに割り当てられる2つの異なる属性はどれですか。 2つ選択してください。）
A. domain
B. IP address
C. DNS server address
D. DHCP server address
E. external spam quarantine
正解: **A,B (**コメントを発表する**)**
Virtual gateways are a feature that allows Cisco ESA to host multiple email domains on a single physical interface, using different IP addresses and hostnames for each domain. When virtual gateways are configured, two distinct attributes are allocated to each virtual gateway address:
Domain, which is the email domain name that is associated with the virtual gateway address, such as mycompany.com or mydomain.com.
IP address, which is the IPv4 or IPv6 address that is assigned to the virtual gateway address, such as 199.209.31.X or 2001:db8::X.
The other options are not attributes that are allocated to each virtual gateway address on Cisco ESA.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118542-qa-esa-00.html

質問: **76**
CiscoESAでのCiscoEメール暗号化の目的は何ですか。
A. 受信者とMTA間の匿名性を確保するため
B. 送信者とMTA間の整合性を確保するため
C. 送信者とCiscoESA間の直接通信を認証するため
D. CiscoESAとMTA間のプライバシーを確保するため
正解: **(**正解を表示します**)**
Overview of Encrypting Communication with Other MTAs:
AsyncOS supports the STARTTLS extension to SMTP (Secure SMTP over TLS).
The TLS implementation in AsyncOS provides privacy through encryption.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_011001.html?bookSearch=true

質問: **77**
ネットワーク管理者は、LDAPサーバーへのクエリが多数あることに気づきました。メールログには、「550無効な受信者が多すぎます外部ホストによって接続が閉じられました」というエントリが表示されます。これに対処するには、どの機能を使用する必要がありますか？
A. DHAP
B. SBRS
C. LDAP
D. SMTP

正解: **A (**コメントを発表する**)**
Directory Harvest Prevention. You can configure the appliance to combat directory harvest attacks using your LDAP directories. You can configure directory harvest prevention during the SMTP conversation or within the work queue. If the recipient is not found in the LDAP directory, you can configure the system to perform a delayed bounce or drop the message entirely.
Consequently, spammers are not able to differentiate between valid and invalid email addresses.
See Using LDAP For Directory Harvest Attack Prevention.
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_011010.html?bookSea rch=true

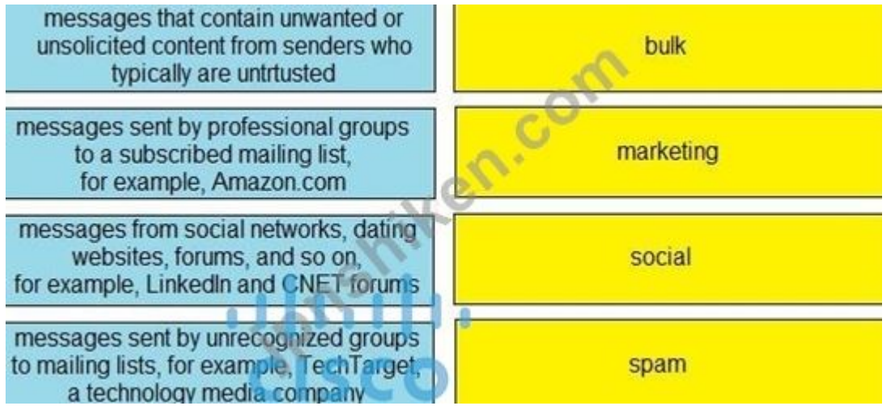
質問: **78**
管理者は、電子メールがドメインの所有者によって送信および承認されるようにCiscoESAを設定する必要があります。このタスクを実行するには、どの2つのステップを実行する必要がありますか？ 2つ選択してください。）
A. キーを生成します。
B. 署名プロファイルを作成します。
C. Mxレコードを作成します。
D. SPF検証を有効にします。
E. DMARCプロファイルを作成します。
正解: **(**正解を表示します**)**
To ensure that emails are sent and authorized by the owner of the domain, the following steps must be performed on Cisco ESA:
Generate keys: Generate DomainKeys Identified Mail (DKIM) keys. DKIM is an email authentication method that allows the recipient to verify that an email was indeed sent by the domain it claims to be from.
Create DMARC profile: DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a policy framework that builds upon SPF and DKIM to provide additional email authentication and reporting capabilities. By creating a DMARC profile, the administrator can define the desired policy for handling emails that fail SPF or DKIM checks and specify how receiving mail servers should handle such emails.
These steps, generating keys and creating a DMARC profile, contribute to ensuring that emails are sent and authorized by the domain owner, providing improved email authentication and verification mechanisms.

質問: **79**
エンジニアは、Cisco Secure Email Gateway 上で、*@cisco.com から送信されたメールがスパム隔離領域に送られないようにする必要があります。Secure Email Gateway では、どのような設定が必要ですか？
A. コンテンツフィルター
B. URLフィルタリング
C. S/MIME
D. セーフリスト
正解: **(**正解を表示します**)**
To guarantee that email from *@cisco.com bypasses spam quarantine, the engineer must configure a safelist. A safelist explicitly allows messages from trusted senders or domains, preventing them from being flagged or quarantined as spam by the antispam engine.

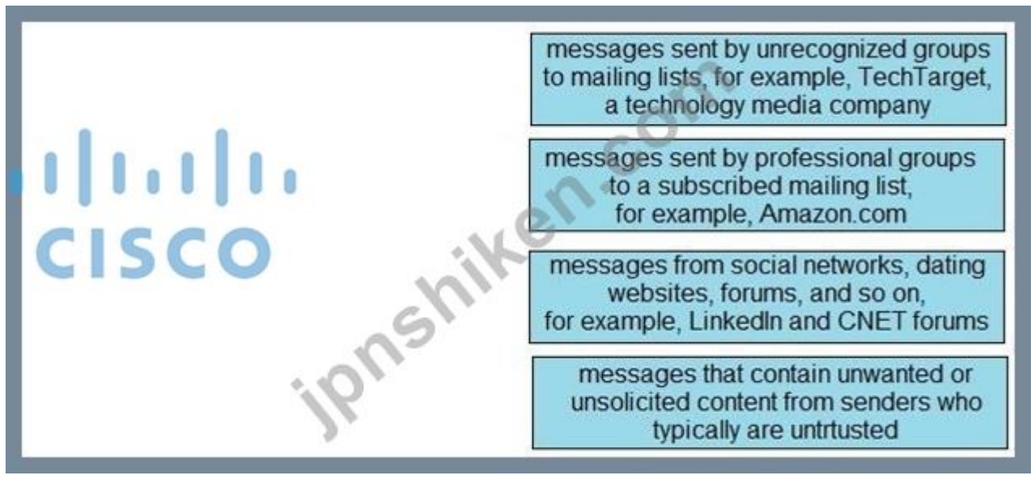
質問: **80**
Cisco ESAの管理者は、複数のメールポリシーを設定しています。特定の送信者を使用してポリシーの一致をテストしたところ、メールが想定されるポリシーと一致しませんでした。
その理由は？
A. 「From」ヘッダーは、すべてのポリシーに対して上から順にチェックされます。

B. 最も優先度の高いメッセージヘッダーが、各ポリシーに対して上から順にチェックされます。
C. 「To」ヘッダーは、すべてのポリシーに対して上から順にチェックされます。
D. 最も優先度の高いメッセージヘッダーが、上から下へ順にデフォルトポリシーと照合されます。
正解: **(**正解を表示します**)**
First Match Wins
Each user (sender or recipient) is evaluated for each mail policy defined the appropriate mail policy table in a top-down fashion.
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?bookSear ch=true

質問: **81**
ドラッグアンドドロップ問題
左側のグレーメールの説明を、右側の該当する評決カテゴリにドラッグアンドドロップしてください。



正解:



質問: **82**
Cisco Secure Email Gateway が S/MIME 暗号化を実行するプロセスの 2 つの異なるフェーズは何ですか? (2つお選びください。)
A. 暗号化された公開鍵をメッセージに添付します
B. セッションキーを使用してメッセージ本文を暗号化します。
C. 暗号化されたメッセージを送信者に送信します

D. 暗号化された対称キーをメッセージに添付します
E. 擬似ランダムセッションキーを作成します。
正解: **B,E (**コメントを発表する**)**
S/MIME encryption on Cisco Secure Email Gateway works in two phases:
- A pseudo-random session key (symmetric key) is created to perform the actual message encryption.
- The message body is encrypted with this session key, ensuring confidentiality.
The session key itself is then encrypted with the recipient's public key, but the core phases of S/MIME encryption are the generation of the session key and the encryption of the message body with it.

質問: **83**
CRESを設定する際、開封確認機能はどこで有効にするのですか？
A. コンテンツフィルタアクションメニュー
B. メールポリシー
C. コンテンツフィルタ条件メニュー
D. 暗号化プロファイルでは
正解: **(**正解を表示します**)**

質問: **84**
メッセージがSPF検証には合格したが、DKIM検証に失敗した。最も可能性の高い原因は何か？
A. 受信者のメールボックスがいっぱいです
B. 署名後にメッセージの内容が変更されました
C. DNS MXレコードが欠落しています
D. スパム対策スキャンによりDKIM署名が削除されました
正解: **(**正解を表示します**)**
DKIM verifies message integrity using a cryptographic signature. If headers or body content are modified after signing, validation fails. SPF may still pass because SPF validates sending server authorization rather than message integrity.

質問: **85**
一元化されたスパム検疫を使用してCisco ESAからCisco SMAに電子メールを配信するデフォルトのポートは何ですか？
A. 8025
B. 6443
C. 6025
D. 8443
正解: **(**正解を表示します**)**
The default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine is 6025. This is the default value for the Port setting in the External Spam Quarantine configuration on Cisco ESA. This port must be open on both Cisco ESA and Cisco SMA for the communication to work.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure-esa-00.html

質問: **86**
Cisco ESAで電子メール認証が設定されている場合、署名プロファイルでどの2つのキータイプを選択する必要がありますか？　2つ選択してください。）
A. DKIM

B. 公開鍵
C. ドメインキー
D. 対称キー
E. 秘密鍵
正解: **A,C (**コメントを発表する**)**
When configuring the ESA under Mail Policy > Sending Profile, the two "Domain Key Type:" are DKIM and Domain Keys.
DKIM (DomainKeys Identified Mail): This is a method for associating a domain name with an email message, thereby allowing a person, role, or organization to claim some responsibility for the message. It is widely used and is the successor to Domain Keys.
Domain Keys: This is an older standard used for email authentication that works similarly to DKIM but has largely been replaced by DKIM. However, Cisco ESA still includes it as an option.

質問: **87**
通知のマージ中にスパム検疫を設定するときに、どのタイプのクエリを設定する必要がありますか？
A. スパム検疫エイリアスルーティングクエリ
B. スパム検疫エイリアス統合クエリ
C. スパム検疫エイリアス認証クエリ
D. スパム検疫エイリアスマスカレードクエリ
正解: **(**正解を表示します**)**
Spam Quarantine Alias Consolidation Query is a type of query that must be configured when setting up the Spam Quarantine while merging notifications on Cisco ESA. This query allows Cisco ESA to consolidate multiple email addresses that belong to the same end user into one entry in the Spam Quarantine, and send only one notification email to that end user with all the quarantined messages for all their email addresses.

質問: **88**
多層アンチウイルススキャンが設定されている場合のウイルススキャンの順序は？
A. デフォルトのエンジンは最初にウイルスをスキャンし、McAfeeエンジンは2番目にウイルスをスキャンします。
B. ソフォスエンジンが最初にウイルスをスキャンし、マカフィーエンジンが次にウイルスをスキャンします。
C. McAfeeエンジンが最初にウイルスをスキャンし、デフォルトのエンジンが2番目にウイルスをスキャンします。
D. McAfeeエンジンが最初にウイルスをスキャンし、次にSophosエンジンがウイルスをスキャンします。
正解: **(**正解を表示します**)**

Scanning Messages with Multiple Anti-Virus Scanning Engines

AsyncOS supports scanning messages with multiple anti-virus scanning engines — multi-layer anti-virus scanning. You can configure your Cisco appliance to use one or both of the licensed anti-virus scanning engines on a per mail policy basis. You could create a mail policy for executives, for example, and configure that policy to scan mail with both Sophos and McAfee engines.

Scanning messages with multiple scanning engines provides "defense in depth" by combining the benefits of both Sophos and McAfee anti-virus scanning engines. Each engine has leading anti-virus capture rates, but because each engine relies on a separate base of technology (discussed in McAfee Anti-Virus Filtering, on page 343 and Sophos Anti-Virus Filtering, on page 340) for detecting viruses, the multi-scan approach can be even more effective. Using multiple scanning engines can lead to reduced system throughput, please contact your Cisco support representative for more information.

You cannot configure the order of virus scanning. When you enable multi-layer anti-virus scanning, the McAfee engine scans for viruses first, and the Sophos engine scans for viruses second. If the McAfee engine determines that a message is virus-free, the Sophos engine scans the message, adding a second layer of protection. If the McAfee engine determines that a message contains a virus, the Cisco appliance skips Sophos scanning and performs actions on the virus message based on settings you configured.

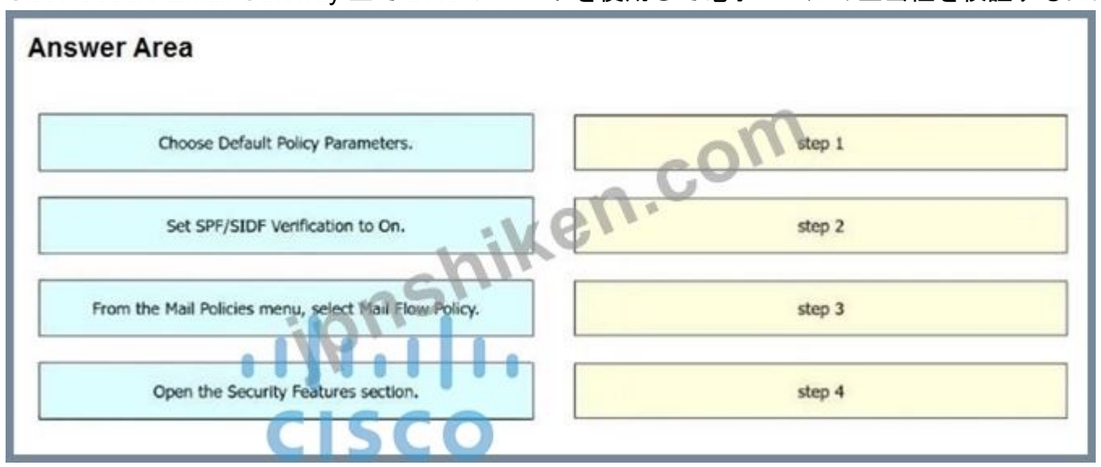
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf P.402

質問: **89**
グレイメール管理ソリューションの構成要素を2つ挙げてください。(2つ選択してください。)
A. クラウドベースの購読解除サービス
B. Sophosベースの購読解除サービス
C. オンプレミス型購読解除サービス
D. 統合型グレイメールスキャンエンジン
E. 複合グレイメールスキャンエンジン
正解: **(**正解を表示します**)**
Graymail management uses an integrated graymail scanning engine to identify graymail categories and a cloud-based unsubscribe service to process unsubscribe requests safely for supported messages.

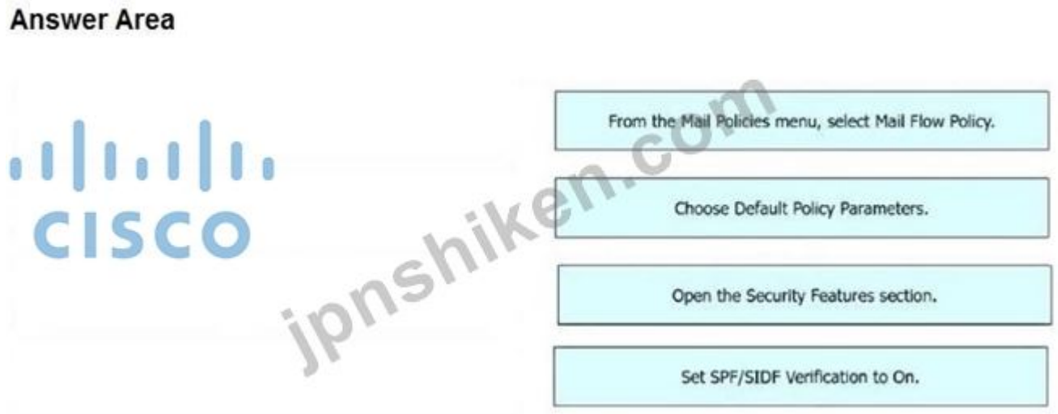
質問: **90**
エンジニアがCisco Secure Email Gatewayを設定中で、user0516585210@acme.comというメールアドレスを持つ受信者へのメールを拒否する必要があります。許可された受信者アドレスが含まれているリストはどれですか？
A. バット
B. 帽子
C. 土
D. ネズミ
正解: **(**正解を表示します**)**

The Recipient Access Table defines which recipient addresses are accepted or rejected during the SMTP conversation, so it is used to control whether messages to a specific recipient address are allowed.

質問: **91**
ドラッグアンドドロップ問題
Cisco Secure Email Gateway 上で DNS レコードを使用して電子メールの正当性を検証するには、左側のアクションを右側の順番にドラッグアンドドロップしてください。



正解:



Explanation:
This order ensures you navigate to the correct mail flow policy, access its parameters, find the security options, and enable DNS-based sender verification for email authenticity.

質問: **92**

Cisco ESA は、無効な受信者に送信されたメッセージを多数処理しています。この過剰な処理を軽減するため、エンジニアは受信者検証に LDAP を使用する準備をしています。このタスクを実行するために必要な 2 つの手順はどれですか？(2 つ選択してください。)
A. LDAPサーバープロファイルを設定します。
B. 外部LDAP認証を有効にする。
C. LDAPクエリを設定します。
D. リスナーで LDAP 認証を有効にします。
E. 受信メールポリシーを設定して、LDAPサーバーにクエリを実行します。
正解: **(**正解を表示します**)**
Directory Harvest Attack Prevention within the SMTP Conversation
You can prevent DHAs by entering only domains in the Recipient Access Table (RAT), and performing the LDAP acceptance validation in the SMTP conversation.
To drop messages during the SMTP conversation, configure an LDAP server profile for LDAP acceptance. Then, configure the listener to perform an LDAP accept query during the SMTP conversation.
Once you configure LDAP acceptance queries for the listener, you must configure DHAP settings in the mail flow policy associated with the listener.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_011011.html?bookSearch=true#con_1163450
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118218-configure-esa-00.html

質問: **93**
アプライアンスがメッセージを受け入れる前に、受信者アドレスが有効かどうかを判断するESAコンポーネントはどれですか？
A. LDAP承認クエリ
B. DKIM認証
C. 送信者検証例外リスト
D. アウトブレイクフィルター
正解: **A (**コメントを発表する**)**
LDAP Acceptance Queries validate recipients against directory services such as Active Directory during the SMTP conversation. Invalid recipients are rejected before message acceptance, reducing processing overhead, preventing directory harvest attacks, and minimizing non-delivery report generation.

質問: **94**
IP インターフェイスの 1 つで割り当てられた証明書が変更された場合、どの機能が影響を受けますか?
A. Cisco Secure Email Gateway と LDAP サーバ間のトラフィック
B. Cisco Secure Email Gateway から配信される電子メール
C. Cisco Secure Email Gateway の Web ユーザ インターフェイスに接続するときの HTTPS トラフィック
D. Cisco Secure Email Gateway によって受信される電子メール
正解: **(**正解を表示します**)**
If the assigned certificate under one of the IP interfaces is modified, then the HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway will be impacted. The administrator must ensure that the certificate is valid and trusted by the browser or client that is used to access the web user interface. Otherwise, the connection may fail or generate a warning message.

質問: **95**
Cisco Secure Email Gatewayで署名プロファイルを作成した後、ドメインキー識別メールを使用して送信メールに署名するには何が必要ですか？
A. 宛先コントロールで設定します。
B. メールフローポリシーでDKIMを有効にします。
C. 送信者ドメインを参照する署名プロファイルで十分です。

D. 送信コンテンツフィルタでDKIMを有効にする。

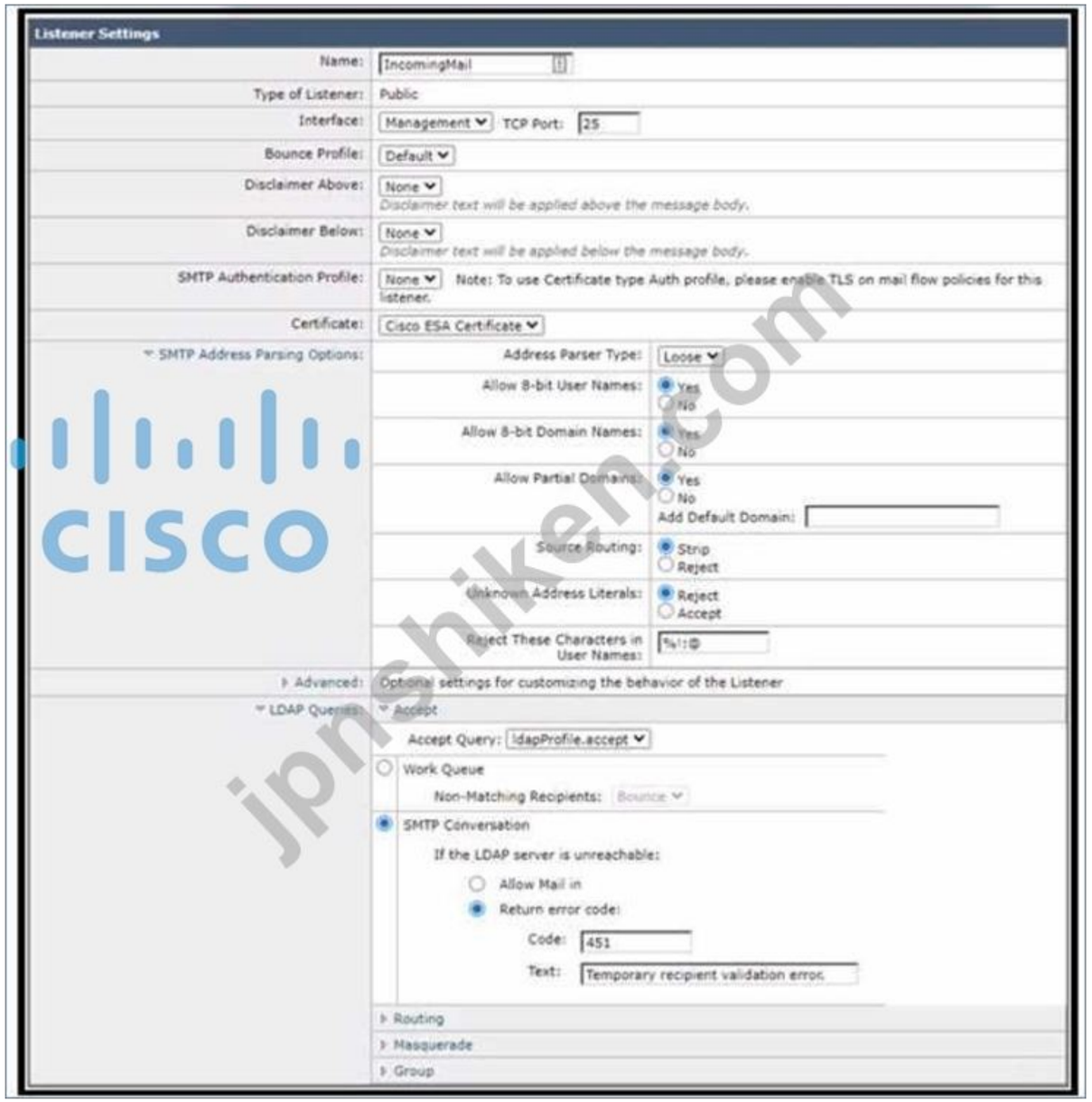
正解: **(**正解を表示します**)**

After creating a signing profile, you must enable DKIM in the mail flow policy for outbound emails.

This ensures that the Cisco Secure Email Gateway signs outgoing messages with DKIM for the specified domains.

質問: **96**

図を参照してください。ディレクトリハーベスト攻撃から保護するために、追加でどのような設定措置を講じる必要がありますか？



A. LDAPクエリが設定されている場合、ディレクトリハーベスト攻撃防止はデフォルトで有効になります。

B. LDAPサーバープロファイルで、ディレクトリハーベスト攻撃防止を設定します。

C. メールフローポリシーで、ディレクトリハーベスト攻撃防止を設定します。
D. リスナー設定で、LDAPクエリ構成を変更してワークキューを使用するように設定します。
正解: **(**正解を表示します**)**
To protect against Directory Harvest Attacks, the administrator must configure Directory Harvest Attack Prevention in the mail flow policy that applies to the listener. This will enable the Cisco Secure Email Gateway to reject or throttle messages that are sent to invalid recipients by checking the LDAP server for valid email addresses.

質問: **97**
DKIM署名が構成されている場合、DKIM公開署名鍵をロードするためにどのDNSレコードを更新する必要がありますか？
A. AAAAレコード
B. PTRレコード
C. TXTレコード
D. MXレコード
正解: **(**正解を表示します**)**
When DKIM (DomainKeys Identified Mail) signing is configured on Cisco ESA, the DNS record that must be updated to load the DKIM public signing key is the TXT record. The TXT record is used to store arbitrary text information in the DNS, such as the DKIM public key, which can be retrieved by the recipients to verify the DKIM signature in the message header.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa-configure-dkim-signing.html

質問: **98**
ドラッグアンドドロップ問題
管理者は、cisco_123@externally.com から送信されるメールが代替仮想ゲートウェイを経由するように設定する必要があります。下部にあるコードスニペットをグラフィックの空白部分にドラッグアンドドロップして、メッセージフィルタ構文を完成させてください。すべてのコードスニペットが使用されるわけではありません。

Envelope-sender ==“cisco_123@externally.com”

mail-from ==“cisco_123@externally.com”

Sender ==“cisco_123@externally.com

delivery-int(“delivery_interface”);

alt-src-host(“delivery_interface”);

正解:

IP Interfaces

Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname	Delete
delivery_interface	10.66.71.121/31	esa.local.lab	
Management	10.66.71.122/24	C680.lab	

```
delivery override:
if mail-from ==“cisco_123@externally.com”
{
delivery-int(“delivery_interface”);
}
.
```

```
Envelope-sender ==“cisco_123@externally.com”
```

```
Sender ==“cisco_123@externally.com
```

```
alt-src-host(“delivery_interface”);
```

質問: **99**
スマート識別子を適用するために使用されるESAの機能はどれですか？
A. RSAデータ損失防止エンジン
B. テキストリソース
C. 暗号化ポリシー
D. コンテンツフィルター
正解: **(**正解を表示します**)**

質問: **100**
ネットワーク管理者が Sophos アンチウイルス エンジンでウイルス スキャンを有効にし、
Cisco ESAには 感染メールを破棄する」オプションがありますが、エンドユーザーからは依然として大量のフィッシングメールが届くという苦情が寄せられています。この問題を解決するにはどうすれば
よいでしょうか？
A. 評判フィルタリングの設定
B. コンテンツフィルタリングの設定
C. アウトブレイクフィルタリングの設定
D. ウイルス対策エンジンを McAfee に変更します。
正解: **(**正解を表示します**)**
Outbreak Filters protects your network from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur.
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_01110.html?bookSear ch=true

質問: **101**
LDAPグループクエリを使用できるCisco ESAの設備はどれですか？(3つ選択してください。)
A. コンテンツフィルター
B. SenderBaseの評判フィルタリング
C. スパム対策設定
D. ネズミ
E. 受信メールポリシー
F. 目的地コントロール
G. 送信者グループ
H. メッセージフィルター

正解: (正解を表示します)

質問: **102**
Cisco ESAで使用できる認証局リストはどれですか。 2つ選択してください。）
A. デフォルト
B. システム
C. ユーザー
D. カスタム
E. テキ
正解: **B,D** (コメントを発表する)
The appliance uses stored trusted certificate authorities that it uses to verify a certificate from a remote domain to establish the domain's credentials. You can configure the appliance to use the following trusted certificate authorities:
Pre-installed list. The appliance has a pre-installed list of trusted certificate authorities. This is called the system list.
User-defined list. You can customize a list of trusted certificate authorities and then import the list onto the appliance.

質問: **103**
エンジニアは、クレジットカード番号などの添付ファイルを検出し、適切な措置が講じられるまで保留するコンテンツフィルタを作成するよう指示されました。この要件を満たすには、Cisco ESA のどのコンポーネントを設定する必要がありますか？
A. スパム隔離
B. アウトブレイクフィルター
C. 政策隔離
D. コンテンツフィルター
正解: **B** (正解を表示します)
Content filter is a component on a Cisco Secure Email Gateway that must be configured to catch attachments, including credit card numbers, and hold them for review until further action is taken.
Content filter allows you to define rules based on message content and apply actions such as quarantine, encrypt, or modify.

質問: **104**
ある企業は最近セキュリティ ポリシーを更新し、外部ソースから送信される 100 MB を超える電子メール メッセージをすべて削除したいと考えています。Cisco Secure Email Gateway は LDAP に統合されており、すべての従業員アカウントは 「従業員」グループに属します。どのフィルタ ルール設定が望ましい結果をもたらしますか?
A. if (グループからのメール == '従業員') および (本文サイズ > "100M") {drop()}
B. if (グループからのメール != '従業員') および (本文サイズ > 100M) {drop();}
C. if (グループからのメール == '従業員') および (本文サイズ > 100M) {bounce();}
D. if ('グループからのメール != 従業員') および (本文サイズ > 100M) {drop();}
正解: **B** (コメントを発表する)
The rule correctly checks whether the sender is not a member of the LDAP "Employees" group and whether the message body size exceeds 100 MB, then drops matching external messages.

質問: **105**
管理者は複数のCiscoESAデバイスを管理しており、中央の場所にあるすべてのデバイスからの検疫電子メールを表示したいと考えています。
これはどのように達成されますか？
A. スパムを外部検疫に送信する前にVOF機能を無効にします。
B. メールポリシーを設定して、メッセージがローカル検疫に送信されるか外部検疫に送信されるかを決定します。
C. SPAMを外部検疫に送信する前に、ローカル検疫を無効にします。

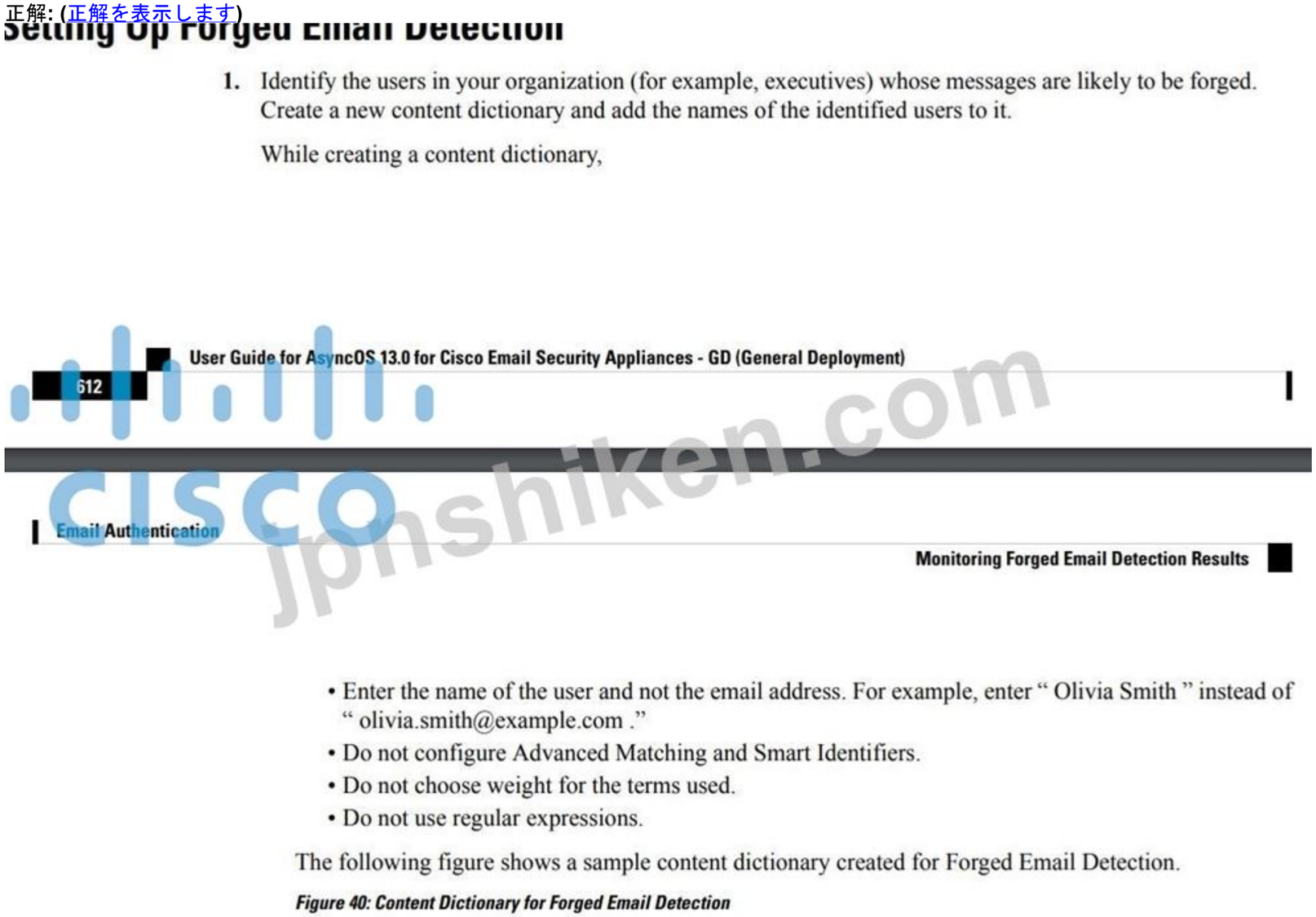
D. メッセージがローカル検疫に送信されるか外部検疫に送信されるかを決定するユーザーポリシーを構成します。
正解: (正解を表示します)
Disabling the Local Spam Quarantine to Activate the External Quarantine If you were using a local spam quarantine before enabling an external spam quarantine, you must disable the local quarantine in order to send messages to the external quarantine.
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_0101010.html?bookSe arch=true#con_1172419

質問: **106**
エンジニアは、メールログを確認して、ドメインabc.comから送信されたメッセージがSPF検証に合格し、CiscoESAによって受け入れられていることを確認する必要があります。エンジニアは、SPF検証が実行されておらず、ドメインabc.comから送信されたメッセージのログでSPFが参照されていないことに気付きました。
検証が正しく機能しないのはなぜですか？
A. 受信者アクセステーブルでSPF検証が無効になっています。
B. メールフローポリシーでSPF検証が無効になっています。
C. SPF適合レベルは、メールフローポリシーでSIDF互換に設定されています。
D. SPF検証コンテンツフィルターが作成されていません。
正解: (正解を表示します)
Enabling SPF and SIDF:
To use SPF/SIDF, you must enable SPF/SIDF for a mail flow policy on an incoming listener. You can enable SPF/SIDF on the listener from the default mail flow policy, or you can enable it for particular incoming mail flow policies.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_010110.html?bookSearch=true#task_1147982

質問: **107**
管理者は、cisco.comとtest.comのように異なるドメインの複数の受信者宛てに送信された特定の添付ファイル付き受信メールが、すべての受信者に配信されないことに気づきました。同じメールをcisco.comの受信者のみに送信した場合は、正しく配信されます。
この動作を回避するには、Cisco ESAをどのように設定する必要がありますか？
A. DLP 設定を変更して、test.com に対してすべての添付ファイルが許可されるようにします。
B. DLP 設定を変更して、test.com ドメインに送信されるメッセージの DLP スキャンを除外します。
C. メール受信者が複数のポリシーに一致しないように、メールポリシーを変更します。
D. cisco.com のメール ポリシーを変更して、メールが破棄されないようにしてください。
正解: (正解を表示します)
By modifying the mail policies, specifically the recipient matching criteria, you can ensure that email recipients do not match multiple policies simultaneously. When recipients in the email message belong to different domains (e.g., cisco.com and test.com), it can result in multiple policies being triggered simultaneously, leading to inconsistent delivery of emails with attachments.
DLP is for outgoing mail only and not relevant to incoming mail.

質問: **108**

アナリストは、偽造メール検出で使用する新しいコンテンツディクショナリを作成します。
辞書に追加されるエントリはどれですか？
A. mycompany.com
B. Alpha Beta
C. ^Alpha\ Beta$
D. Alpha.Beta@mycompany.com
正解: (正解を表示します)



Setting Up Forged Email Detection

1. Identify the users in your organization (for example, executives) whose messages are likely to be forged. Create a new content dictionary and add the names of the identified users to it.

   While creating a content dictionary,

- Enter the name of the user and not the email address. For example, enter " Olivia Smith " instead of " olivia.smith@example.com ."
- Do not configure Advanced Matching and Smart Identifiers.
- Do not choose weight for the terms used.
- Do not use regular expressions.

The following figure shows a sample content dictionary created for Forged Email Detection.

Figure 40: Content Dictionary for Forged Email Detection

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.pdf p.675

質問: **109**
Cisco ESAに望ましくないURL保護を実装するための2つの前提条件は何ですか？ 2つ選択してください。）
A. アウトブレイクフィルターを有効にします。
B. メールリレーを有効にします。

C. スパム対策スキャンを有効にします。
D. ポートのバウンスを有効にします。
E. ウイルス対策スキャンを有効にします。
正解: **(**正解を表示します**)**
Undesirable URL protection is a feature that allows Cisco ESA to detect and block messages that contain URLs that lead to malicious or unwanted websites, such as phishing, malware, or adult content sites. To enable this feature, outbreak filters and antispam scanning must be enabled on Cisco ESA.
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

質問: **110**
最近のエンジンアップデートがgraymailのためにプルダウンされ、サービスがクラッシュし始めました。これをできるだけ早く修正することが重要です。
この問題に対処するには何をする必要がありますか？
A. [サービスの概要]ページから以前のバージョンのエンジンにロールバックします。
B. [システムヘルス]ページから以前のバージョンのエンジンにロールバックします。
C. IMSおよびGraymailページから別の更新をダウンロードします。
D. [サービスの更新]ページから別の更新をダウンロードします。
正解: **(**正解を表示します**)**
The Services Overview page lists the current service and rule versions of the following engines:
Graymail
McAfee
Sophos
You can perform the following tasks in the Services Overview page:
Manually update the engines. For more information, see Manually Updating the Engines Rollback to previous version of the engine. For more information, see Rollback to Previous Version of Engine
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_0100010.html

質問: **111**
ある遠隔地の金融機関がメール暗号化を導入しようとしています。受信メールはすべてTLS経由のSMTPを使用することが義務付けられています。これを実現するにはどうすればよいでしょうか？
A. TLS証明書を無効にします。
B. Cisco Registered Envelope Serviceを利用する。
C. Cisco Talos脅威インテリジェンスグループを活用する。
D. SMTP のアプリケーション検査と制御を有効にします。
正解: **(**正解を表示します**)**
Using TLS Delivery
Transport Layer Security (TLS) delivery allows Encryption Service-originated messages such as secure replies to be delivered encrypted back to the sending domain without having to use an envelope.
You can enable TLS delivery to provide a secure method of delivering email without requiring end users to log in to Encryption Service or install the encryption plug-in to receive or view email.
TLS is enabled on a per-account basis. For each account, you specify one or more TLS domains and error handling behavior.
Note:
From Encryption Service 5.4.1 release onwards, there is no support for domains with only TLS
1.0 enabled for mail delivery. You need to migrate to TLS 1.1 or higher.
https://www.cisco.com/c/en/us/td/docs/security/email_encryption/olh/admin/b_Admin_Guide_lates t/b_Admin_Guide_chapter_0100.html#con_7787262