Cisco.300-720J.v2022-11-12.q34

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：	34
バージョン：	v2022-11-12
ページの閲覧量：	450
問題集の閲覧量：	2561

https://www.jpnshiken.com/shiken/Cisco.300-720J.v2022-11-12.q34.html

質問: **1**
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。
B. ドメインを許可リストに追加します。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **2**
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. SpamCopレピュテーションフィルタリング
B. Talosレピュテーションフィルタリング
C. SenderBaseレピュテーションフィルタリング
D. 接続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**)**

質問: **3**
LDAPグループクエリを使用できるCiscoESA機能の3つのオプションはどれですか。（3つ選択してください。）
A. メッセージフィルター
B. スパム対策設定
C. RAT
D. 宛先コントロール
E. コンテンツフィルター
F. SenderBaseレピュテーションフィルタリング
G. 受信メールポリシー
H. 送信者グループ
正解: **(**正解を表示します**)**

質問: **4**
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. ポートのバウンスを有効にします。
B. ウイルス対策スキャンを有効にします。
C. メールリレーを有効にします。
D. スパム対策スキャンを有効にします。
E. アウトブレイクフィルターを有効にします。
正解: **D,E (**コメントを発表する**)**

質問: **5**
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. データ損失防止
B. ウイルス対策
C. スパム対策
D. 隔離脅威レベル
正解: **(**正解を表示します**)**

質問: **6**
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: **(**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_011010.html

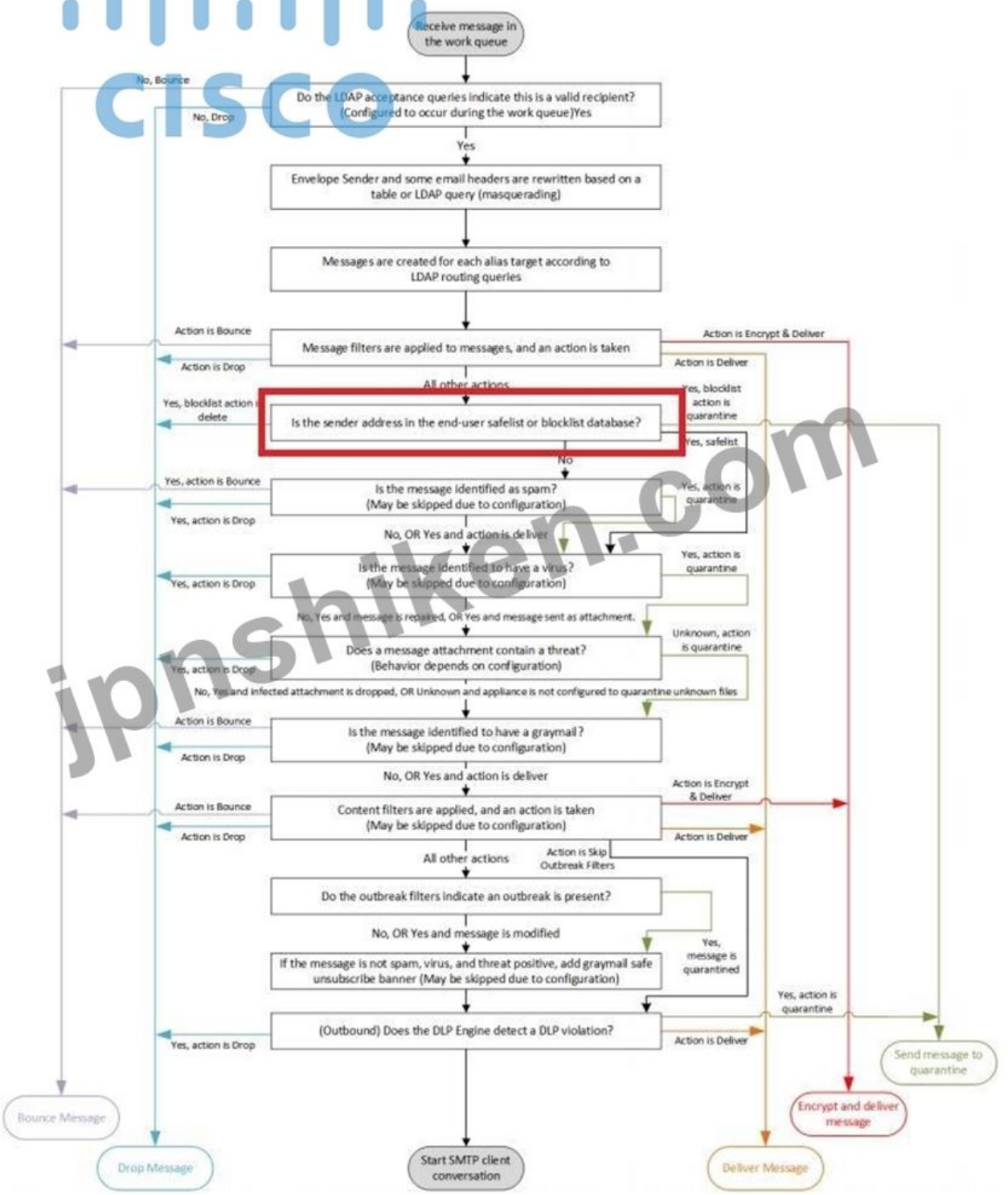
質問: **7**
セーフリストにあるsafedomain.comからメールを受信したときにスキップされるプロセスはどれですか。
A. メッセージフィルター
B. ウイルス対策スキャン
C. アウトブレイクフィルター
D. スパム対策スキャン
正解: **D (**コメントを発表する**)**

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.

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.978
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**: 8**
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ない隔離を削除します。
B. 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。
C. フィルターに割り当てられている隔離を削除します。

D. 未使用の検疫のみを削除します。
正解: **(**正解を表示します**)**

質問: **9**
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. から
B. メッセージID
C. URLレピュテーション
D. 送信者
E. メール差出人
正解: **(**正解を表示します**)**

質問: **10**
次のタイプのDNSレコードのうち、特定のドメインのメール配信を処理するのはどれですか？
A. PTR
B. TXT
C. A
D. MX
正解: **(**正解を表示します**)**

質問: **11**
DLPスキャンを実行するには、どの2つのコンポーネントを構成する必要がありますか？　2つ選択してください。）
A. 送信メールポリシーでDLPポリシーを有効にします。
B. DLPポリシーマネージャーにDLPポリシーを追加します。
C. DLPポリシーのカスタマイズでDLPポリシーを有効にします。
D. DLPポリシーを送信コンテンツフィルターに追加します。
E. 受信メールポリシーにDLPポリシーを追加します。
正解: **A,B (**コメントを発表する**)**

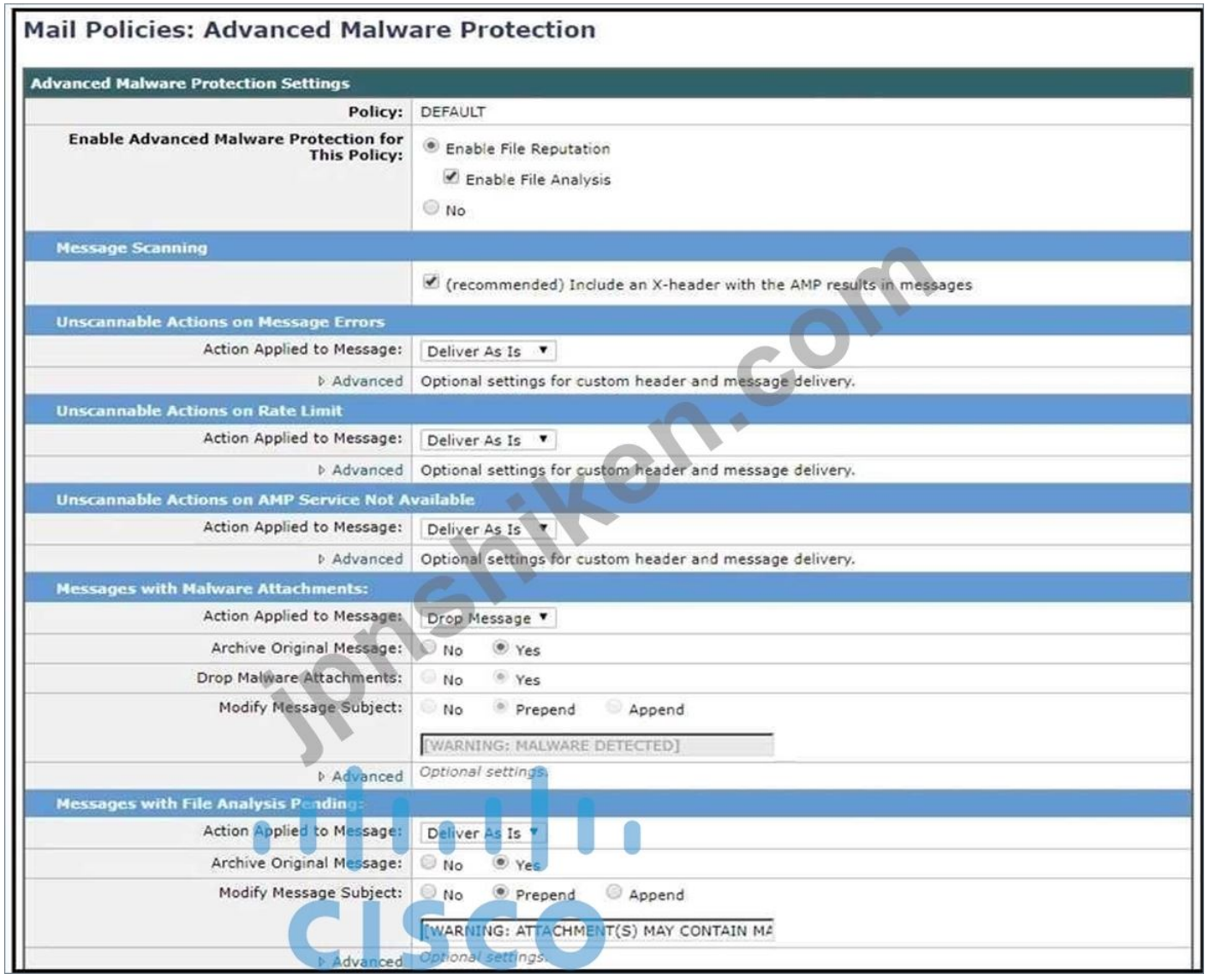
質問: **12**
展示を参照してください。フィルタ2をアクティブに設定するコマンドの正しい順序は何ですか？

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

A. フィルター–詳細–>2-> 1
B. フィルター–変更–すべて–>アクティブ
C. フィルター–編集–>2–>アクティブ
D. フィルター–セット–>2-> 1
正解: **(**正解を表示します**)**

質問: **13**
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. 8443
B. 6443
C. 8025
D. 6025
正解: **D (**コメントを発表する**)**

質問: **14**
展示を参照してください。ゼロデイマルウェア攻撃の配信を停止するには、この構成をどのように変更する必要がありますか？



A. マルウェアの添付ファイルの下にあるメッセージの件名の変更にプリペンドを適用します。

B. ファイル分析の保留中のアクションを[現状のまま配信]から[隔離]に変更します。
C. メールボックスの自動修復を構成します。
D. スキャンできないアクションを[現状のまま配信]から[隔離]に変更します。
正解: **C** (コメントを発表する)

質問: **15**
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. 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
B. 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
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)

質問: **16**
Cisco ESAメッセージフィルターによって実行される2つのアクションタイプはどれですか。 2つ選択してください。）
A. アクションを破棄
B. 非最終アクション
C. 検疫アクション
D. フィルター操作
E. 最終アクション
正解: (正解を表示します)

質問: **17**
Cisco ESAでのSMTP認証中にクライアント証明書が使用できない場合、有効なフォールバックはどのアクションですか？
A. LDAPクエリ
B. LDAPバインド
C. SMTP認証
D. SMTP TLS
正解: (正解を表示します)

質問: **18**
Cisco ESAがアンチウイルススキャンを実行するように設定されている場合、デフォルトのタイムアウト値は何ですか。

Note If a policy quarantine is not defined in your appliance, you cannot sent the message to the quarantine.

You can perform the following additional actions, if you choose to send the message to the policy quarantine:

- Modify the message subject
- Add a custom header to the message

A. 120秒
B. 30秒
C. 90秒
D. 60秒
正解: **(**正解を表示します**)**

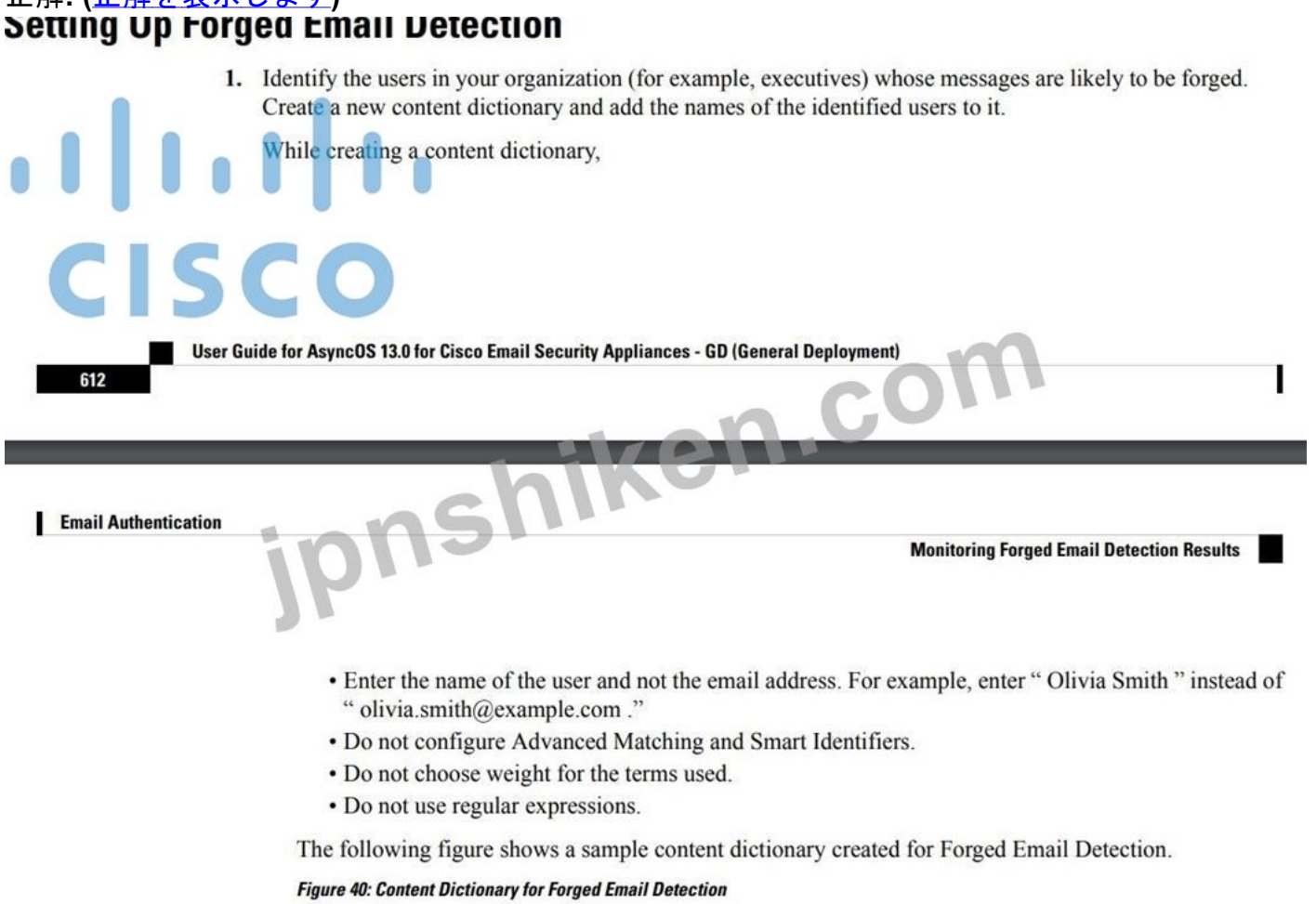
質問: **19**
エンジニアは初めてCiscoESAを設定し、内部SMTPサーバからの電子メールトラフィックがCisco ESAを介して中継され、送信メールポリシーに関連付けられていることを確認する必要があります。
この目標を達成するには、どのメールフローポリシー設定を変更する必要がありますか？
A. 例外リスト
B. 接続動作
C. バウンス検出署名
D. 逆接続検証
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html

質問: **20**
ある会社は、営業部門から外部に送信されたすべての電子メールをDLPでスキャンしてPCI-DSSに準拠することを要求する新しいマンデートを展開しました。新しいDLPポリシーがCiscoESAで作成されており、まだ作成されていない「Sales」という名前のメールポリシーに割り当てる必要があります。
このタスクを実行するには、どのメールポリシーを作成する必要がありますか？
A. 送信メールポリシー
B. 予備のメールポリシー
C. 受信メールフローポリシー
D. 送信メールフローポリシー
正解: **A (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html#task_14094

質問: **21**
受信メールポリシーまたは送信メールポリシーに適用される2つの機能はどれですか。 2つ選択してください。）

A. アウトブレイクフィルター
B. アプリケーションフィルタリング
C. 侵害の兆候
D. 送信者評価フィルタリング
E. ウイルス対策
正解: **A,E** (コメントを発表する)

質問: **22**
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,

cisco

User Guide for AsyncOS 13.0 for Cisco Email Security Appliances - GD (General Deployment)
612

jpnshiken.com

Email Authentication
Monitoring Forged Email Detection Results

- 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.

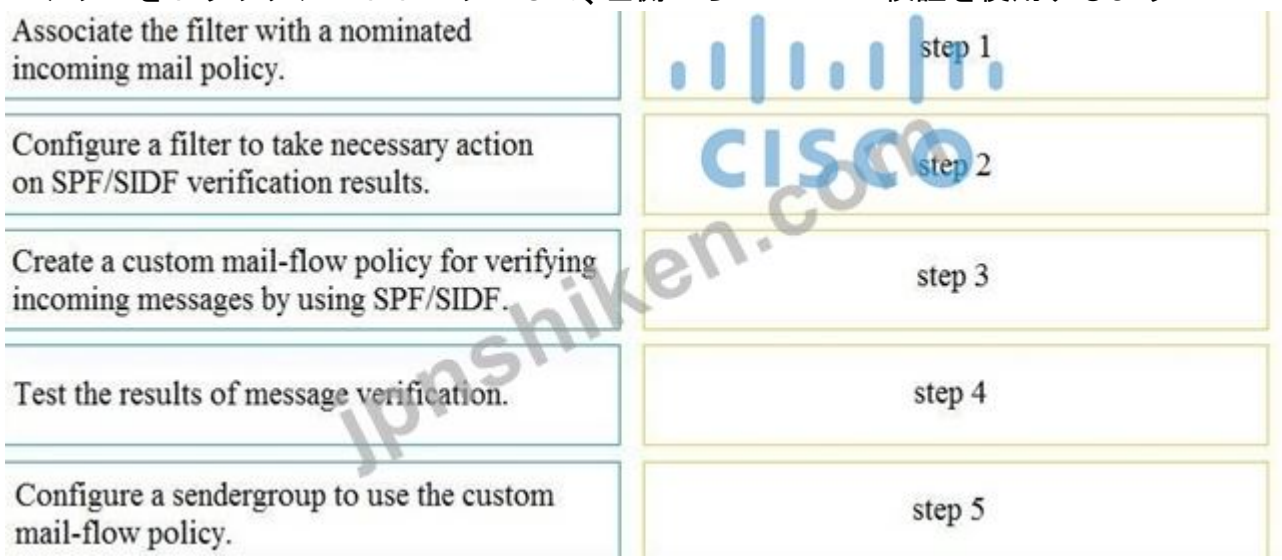
Figure 40: Content Dictionary for Forged Email Detection

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

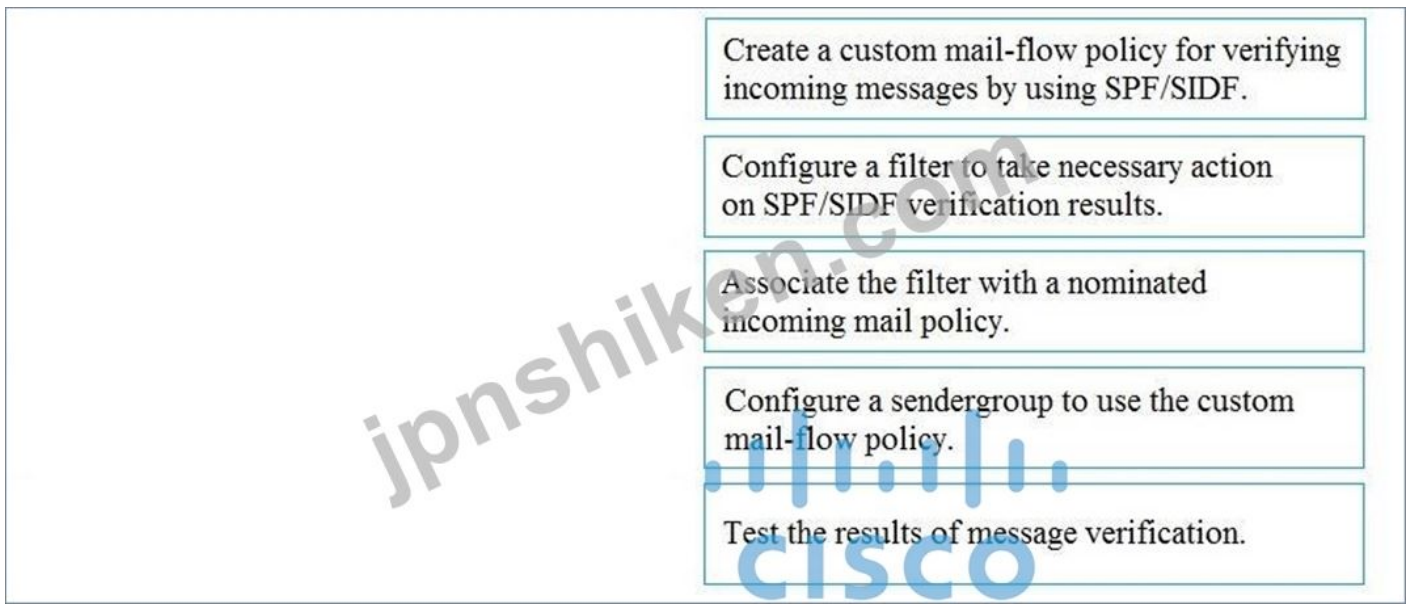
質問: **23**
個別の受信メールポリシーを設定するとどうなりますか？
A. メッセージの分裂

B. メッセージの例外
C. メッセージ集約
D. メッセージの分離
正解: **(**正解を表示します**)**

質問: **24**
ドラッグアンドドロップの質問
ステップをドラッグアンドドロップして、左側からSPF /SIDF検証を使用するようにCiscoESAを設定し、右側の正しい順序に配置します。



正解:



質問: **25**
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. active-active
C. SLA monitor
D. failover
E. active-standby

正解: **A,D** (コメントを発表する)

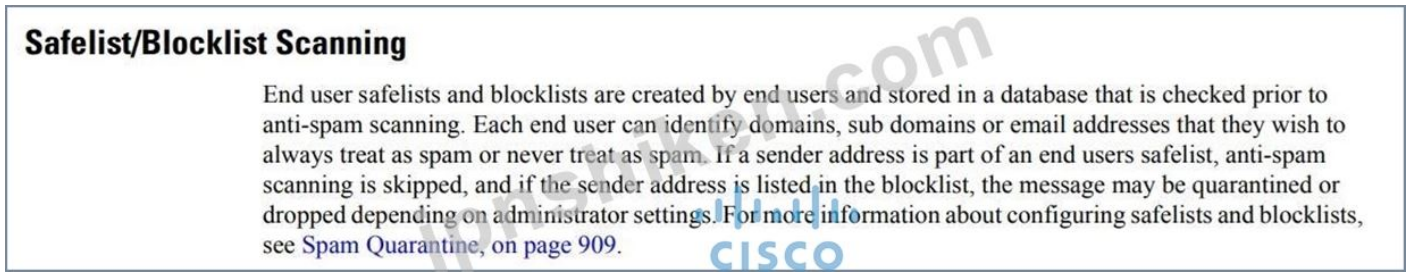
質問: **26**
通知のマージ中にスパム検疫を設定するときに、どのタイプのクエリを設定する必要がありますか？
A. スパム検疫エイリアス統合クエリ
B. スパム検疫エイリアスルーティングクエリ
C. スパム検疫エイリアス認証クエリ
D. スパム検疫エイリアスマスカレードクエリ
正解: (正解を表示します)

質問: **27**
管理者は、SPFがメッセージを確認し、信頼できるパートナーが誤ってDNS設定を誤って構成したかどうかを判断するのに失敗するすべてのメッセージを隔離するために、コンテンツフィルターを作成しました。管理者は、24時間後にメッセージを解放するようにポリシー検疫を設定し、ビジネスを中断せずに確認できるようにします。
エンドユーザーがこれらのメッセージを操作するリスクが高いことを認識できるようにするには、どの追加オプションを使用する必要がありますか？
A. アタッチメントを剥がす
B. 受信者に通知する
C. 件名を変更
D. 送信者に通知
正解: (正解を表示します)

質問: **28**
Cisco ESA内のメッセージフィルターの構成について正しい2つの文はどれですか。 2つ選択してください。）
A. Webユーザーインターフェイス内のメッセージフィルター構成は、受信コンテンツフィルター内にあります。
B. メッセージフィルターは、Webユーザーインターフェイスからのみ構成できます。
C. メッセージフィルターは、CLIからのみ構成できます。
D. CLIから実行されるfiltersコマンドは、メッセージフィルターの設定に使用されます。
E. CLIから実行されるfilterconfigコマンドは、メッセージフィルターの構成に使用されます。
正解: (正解を表示します)

質問: **29**
SPAM検疫を実装するときに、組織は何に対処しようとしていますか？
A. true positives
B. false negatives
C. false positives
D. true negatives
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_0100000.html#con_ 1482874

質問: **30**
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: **D** (コメントを発表する)


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: **31**
Cisco ESAでスパム検疫を設定するときのデフォルトのHTTPSポートは何ですか？
A. 80
B. 82
C. 83
D. 443
正解: (正解を表示します)

質問: **32**
Cisco ESAでスパム検疫が設定されている場合、エンドユーザー検疫へのログイン中にLDAPを介してエンドユーザーを検証するものは何ですか？
A. スパム検疫エイリアス統合クエリ
B. スパム検疫外部認証クエリ
C. スパム検疫エンドユーザー認証クエリ
D. エンドユーザーセーフリスト/ブロックリスト機能を有効にする
正解: (正解を表示します)

質問: **33**
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: **34**
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. Mxレコードを作成します。
C. 署名プロファイルを作成します。
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**)**