Cisco.300-720J.v2026-10-08.q85

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：	85
バージョン：	v2026-10-08
ページの閲覧量：	106
問題集の閲覧量：	861

https://www.jpnshiken.com/shiken/Cisco.300-720J.v2026-10-08.q85.html

質問: **1**
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暗号化を適用する簡単な方法を備えている必要があります。Cisco Secure Email Gateway アプライアンスがすべてのメッセージをスキャンし、検出によって自動的に暗号化するのではなく、暗号化が必要なメッセージにユーザがフラグを付けることができる必要があります。この機能を有効にするアクションはどれですか?
A. 件名設定を[SECURE]に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する
B. 条件を指定せず、件名設定で [SECURE] を設定して暗号化して今すぐ配信するアクションを使用して、送信コンテンツ フィルターを作成します。
C. 暗号化プロファイルと、件名ヘッダー内に \[SECURE\] を含む送信コンテンツ フィルターを作成します。暗号化して今すぐ配信するアクションとともに条件が含まれます
D. 暗号化を有効にして DLP ポリシー マネージャーのメッセージ アクションを作成し、それを送信メールのアクティブな DLP ポリシーに適用します。
正解: **(**正解を表示します**)**
According to the [Cisco Secure Email Encryption Service Add-In User Guide], you can create an encryption profile that defines the encryption settings and options for your encrypted messages[2, p. 11]. You can also create an outgoing content filter that applies the encryption profile to the messages that match certain conditions, such as having [SECURE] in the subject header[2, p. 12]. This way, you can allow users to flag the messages that require encryption by adding [SECURE] to the subject line.
The other options are not valid because:
A) Creating an encryption profile with [SECURE] in the Subject setting and enabling encryption on the mail flow policy will not work, as the Subject setting in the encryption profile is used to specify the subject line of the encrypted message envelope, not the original message[2, p. 11].
B) Creating an outgoing content filter with no conditions and with the Encrypt and Deliver Now action configured with [SECURE] in the Subject setting will not work, as this will encrypt all outgoing messages regardless of whether they have [SECURE] in the subject line or not[2, p. 12].
D) Creating a DLP policy manager message action with encryption enabled and applying it to active DLP policies for outgoing mail will not work, as this will encrypt messages based on DLP rules that detect sensitive data in the message content, not based on user flags in the subject line.

質問: **2**
展示を参照してください。

Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering:	☑ Enable File Reputation
File Analysis: ?	☑ Enable File Analysis

☑ Select All Expand All Collapse All Reset

- ☑ **Archived and compressed**
- ☑ **Configuration**
- ☑ **Database**
- ☑ **Document**
- ☑ **Email**
- ☑ **Encoded and Encrypted**
- ☑ **Executables**
- ☑ **Microsoft Documents**
- ☑ **Miscellaneous**

▾ Advanced Settings for File Reputation	File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)
	AMP for Endpoints Console Integration ?	Register Appliance with AMP for Endpoints
	SSL Communication for File Reputation:	☐ Use SSL (Port 443) Tunnel Proxy (Optional): Server: Port: Username: Passphrase: Retype Passphrase: ☐ Relax Certificate Validation for Tunnel Proxy ?
	Heartbeat Interval:	15 minutes
	Query Timeout:	15 seconds
	Processing Timeout:	120 seconds
	File Reputation Client ID:	acd198c2-7ba5-4015-bb20-84ec4590a2ef
	File Retrospective:	☐ Suppress the verdict update alerts ?
▸ Advanced Settings for File Analysis	*Advanced settings for File Analysis*	
▸ Cache Settings	*Advanced settings for Cache*	
▸ Threshold Settings	*Advanced Settings for File Analysis Threshold Score*	

Cancel Submit

```
Mon Aug 12 18:57:58 2019 Warning:   MID 0 reputation query failed for attachment 'amp_watchdog.txt' with error "Cloud query failed"
Mon Aug 12 18:57:58 2019 Info:   Response received for file reputation query from [n/a]. File Name = 'amp_watchdog.txt', MID = 0, Dispositi
on = UNSCANNABLE, Malware = None,  Reputation Score = 0, sha256 = , upload_action = 2
Mon Aug 12 18:57:58 2019 Info:   The attachment could not be scanned. File Name = 'amp_watchdog.txt', MID = 0, SHA256 =, Unscannable Catego
ry = Service Not Available, Unscannable Reason = File Reputation service not available
Mon Aug 12 18:58:55 2019 Warning:   The File Reputation service is not reachable.
```

```
(Machine ESA_1.cisco.com) (SERVICE)> telnet cloud-sa.amp.cisco.com 443
```

jpnshiken.com
CISCO

```
Trying 52.21.117.50...
Connected to ec2-52-21-117-50.compute-1.amazonaws.com.
Escape character is '^]'.
```

管理者は Cisco Secure Email Gateway アプライアンスでファイル レピュテーションとファイル分析を設定しましたが、期待どおりに機能しません。これが機能するには、アプライアンスで何を設定する必要がありますか?

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 Secure Email Gateway にアップロードします。
B. Cisco Secure Email Gateway 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のポート 443 を開きます。
C. ファイル レピュテーション サーバへの接続に SSL を使用するように Cisco Secure Email Gateway を設定します。
D. 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 エンジンをファイル レピュテーション クラウドに強制的に接続します。
正解: (正解を表示します)
To enable File Reputation and File Analysis on the Cisco Secure Email Gateway appliance, the administrator must configure the appliance to use SSL for the connection to the File Reputation server. This wi ll ensure that the communication between the appliance and the cloud service is secure and encrypted. The administrator must also upload a valid certificate from a trusted CA on the appliance for this purpose. The other options are not required or effectiv e for this task. References : [Cisco Secure Email Gateway Administrator Guide - Configuring File Reputation and File Analysis]

質問: **3**

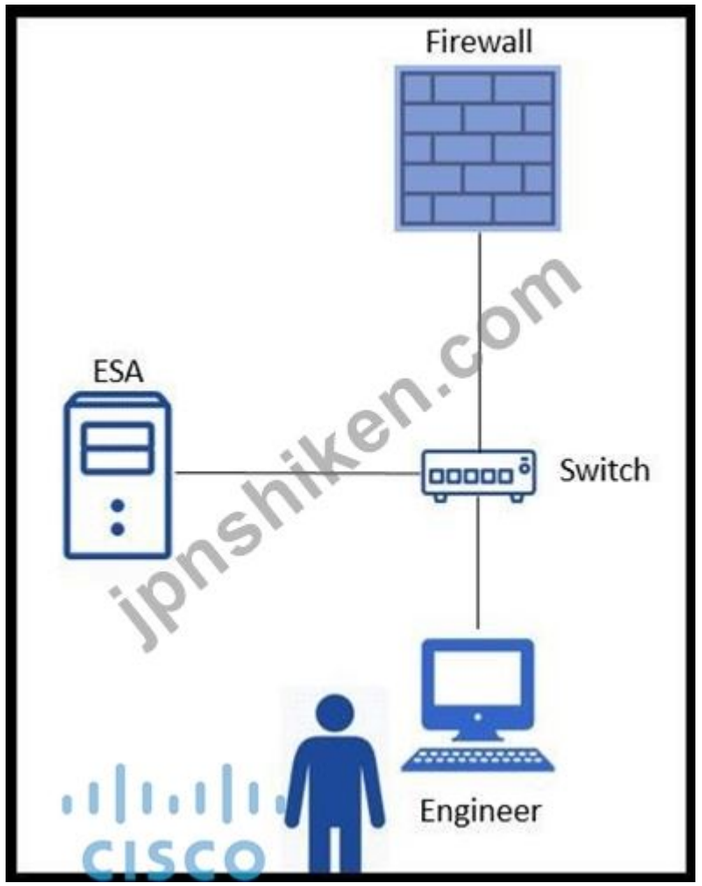
Num	Active	Valid	Name
1	Y	Y	Anti_Spoofing
2	N	Y	Skip-filter
3	Y	Y	WHITELIST

jpnshiken.com

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？

A. filters- > edit- > 2- > Active
B. filters- > modify- > All- > Active
C. filters- > detail- > 2- > 1
D. filters- > set- > 2- > 1
正解: (正解を表示します)
The correct order of commands to set filter 2 to active on the CLI of Cisco ESA is:
* filters, which enters the message filter mode.
* set, which sets the status of one or more message filters.
* 2, which specifies the message filter number.
* 1, which sets the status of message filter 2 to active.
The other options are not valid orders of commands to set filter 2 to active on the CLI of Cisco ESA, because they use incorrect commands or parameters.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page A-6 and page A-7.

質問: **4**



jpnshiken.com

図を参照してください。エンジニアがSSHを使用してCisco E SAに接続しようとしていますが、接続に失敗しています。
さらに調査を進めた結果、エンジニアは隣接するスイッチとの接続が途切れていることに気づいた。
設定上の問題を特定するには、どの接続方法を使用すべきでしょうか？
A. Telnet
B. HTTPS
C. イーサネット
D. シリアル
正解: **D** (コメントを発表する)
Serial connection is a method that should be used to determine the configuration issue when there is a loss of connectivity to the neighboring switch. Serial connection allows the engineer to access the Cisco ESA console port using a serial cable and a terminal emulator, such as PuTTY or HyperTerminal, without relying on the network connectivity.
The other options are not valid methods to determine the configuration issue when there is a loss of connectivity to the neighboring switch, because they require network connectivity to work.
References: Cisco Email Security Appliance C690 Quickstart Guide , page 2.

質問: **5**
Cisco ESA管理者には、いくつかのメールポリシーが設定されています。特定の送信者を使用してポリシーの一致をテストしているときに、電子メールが期待されるポリシーと一致していませんでした。
これの理由は何ですか？
A. Tram *ヘッダーは、トップダウン方式ですべてのポリシーに対してチェックされます。
B. 優先度が最も高いメッセージヘッダーが、トップダウン方式で各ポリシーに対してチェックされます。

C. To "ヘッダーは、トップダウン方式ですべてのポリシーに対してチェックされます。
D. 優先度が最も高いメッセージヘッダーが、トップダウン方式で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)
The envelope sender and the envelope recipeint have a higher priority over the sender header when you match a message to a mail policy. If you configure a mail policy to match a specific user, the messages are automatically classified into the mail policy based on the envelo pe sender and the envelope recipient.
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

質問: **6**
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. 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。
B. 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。
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. システム管理からメッセージの分割を有効にします。
E. 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。
正解: (正解を表示します)

質問: **7**
Cisco ESAのスキャン動作のアクションとしてメッセージが隔離に送信されないのはどのシナリオですか？
A. ポリシー検疫がありません。
B. 複数のメールパイプラインが定義されています。
C. 「メッセージの件名を変更する」はすでに設定されています。
D. 「カスタムヘッダーの追加」アクションが最初に実行されます。
正解: (正解を表示します)
A policy quarantine is a type of quarantine that allows Cisco ESA to store messages that match certain criteria, such as virus, spam, or DLP verdicts, for further review or release by an administrator or an end user.
A scenario that prevents a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA is when a policy quarantine is missing, which means that no policy quarantine has been created or enabled on Cisco ESA.
The other options do not prevent a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-2 and page 10-3.

質問: **8**
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)
The safelist is a list of email addresses or domains that are considered legitimate and trustworthy by Cisco ESA. When an email is received from a sender on the safelist, Cisco ESA skips

antispam scanning for that message and delivers it to the recipient without any spam filtering.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-13.

質問: **9**
CEO は、123ABCDEFGHJ という文字列を含むすべての電子メールは配信できないため、さらなる検査のために隔離する必要があることを示す電子メールを送信しました。要件を考慮すると、その基準に一致させるにはどの正規表現を使用する必要がありますか?
A. \\D{3}[AZ]{9}
B. \d{3}[AZ]{9}
C. \W{3}[AZ]{9}
D. {3}\d{9}[AZ]
正解: **(**正解を表示します**)**
A regular expression is a sequence of characters that defines a search pattern for text. To match a string of
123ABCDEFGHJ, you need to use the following regular expression: \d{3}[A-Z]{9}. This expression means that the string must start with three digits (\d{3}), followed by nine uppercase letters ([A-Z] {9}). This expression will match any string that has the sam e format as 123ABCDEFGHJ. References = User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Regular Expressions
[Cisco Secure Email Gateway] - Cisco

質問: **10**
ユーザーは、冒とく的な表現を含むメールの量が多いことに不満を持っています。ネットワーク管理者は、辞書を活用し、不適切な電子メールの数を減らすために特定の条件を作成する必要があります。
これに対処するために構成する必要がある2つのフィルターはどれですか？ 2つ選択してください。）
A. メッセージ
B. スパム
C. VOF
D. 送信者グループ
E. コンテンツ
正解: **(**正解を表示します**)**
Message filter and content filter are two filters that should be configured to address this issue. Message filter and content filter are rules that allow Cisco ESA to perform actions on messages based on predefined or custom conditions, such as headers, envelope, body, attachments, etc.
To reduce the number of inappropriate emails containing profanity, the network administrator can create a dictionary that contains a list of profane words or phrases and use it as a condition in a message filter or content filter that applies an action of "drop", "quarantine", or "modify subject" on the matching messages.
The other options are not valid filters to address this issue, because they do not use dictionaries or conditions based on message content.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 8-3 and page 8-7.

質問: **11**
アウトブレイク フィルターは、フィッシング詐欺やマルウェア配布サイトなどの小規模で非ウイルス性の攻撃を阻止するためにどのようなアクションを実行しますか?
A. URL を書き換えて、Web セキュリティ プロキシを通じてトラフィックを有害な可能性のある Web サイトにリダイレクトします。
B. 有害な可能性のある Web サイトに関連付けられた電子メール ドメインからのすべての電子メールをブロックします。
C. 有害な可能性のある Web サイトに関連付けられた電子メール ドメインからすべての添付ファイルを削除します。
D. 有害な可能性のある Web サイトへのリンクを含むメッセージを、サイトがオフラインになるまで隔離します。
正解: **(**正解を表示します**)**

Outbreak Filters can take the action of rewriting URLs to redirect traffic to potentially harm ful websites through a web security proxy. This allows the Cisco Secure Email Gateway to scan the content of the websites and block or warn the user if they are malicious or undesirable. This action can stop small-scale and nonviral attacks, such as phishi ng scams and malware distribution sites, that may not be detected by other filters. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Outbreak Filters]

質問: **12**
Cisco ESAスキャン動作で構成されるグローバル設定はどれですか？
A. スキャンする添付ファイルの最小サイズ
B. 添付ファイルのスキャンのタイムアウト
C. 添付ファイルの種類が原因でスキャンできないメッセージに対するアクション
D. スキャンする添付ファイルの再帰の最小深度
正解: (正解を表示します)
The global setting that is configured under Cisco ESA Scan Behavior is the actions for unscannable messages due to attachment type. This setting allows the administrator to specify what action to take when a message contains an attachment that cannot be scanned by the appliance, such as encrypted or password-protected files. The possible actions are:
* Deliver - Deliver the message normally.
* Drop - Drop the message silently without notifying the sender or recipient.
* Quarantine - Quarantine the message in a specified policy quarantine.
* Bounce - Bounce the message back to the sender with a specified reason.
Reference:
Scan Behavior
Reference: https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scan-behavior- impact-on-av/td-p/3923243

質問: **13**
ネットワーク管理者は、会社の従業員が社外にクレジットカード情報を送信できないようにするために、どの事前定義されたDLPカテゴリを使用する必要がありますか？
A. 企業機密
B. 知的財産保護
C. 許容される使用
D. 規制遵守
正解: (正解を表示します)

質問: **14**
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.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-2.

質問: **15**

管理者は、アプライアンスの Cisco Secure Email Gateway 配信キューが常にいっぱいであることに気づきました。さらに調査した結果、アプライアンスで現在使用されている IP アドレスが一部の宛先でレート制限されていることが判明しました。管理者は、仮想ゲートウェイ技術を使用して追加の IP アドレスを持つ新しいインターフェイスを作成しましたが、問題は解決されません。どの構成変更によって問題が解決されますか?

A. CLI コマンド altsrchost を使用して、新しいインターフェイスをすべてのメールの送信元 IP アドレスとして設定します。

B. CLI コマンドloadbalance auto を使用して、すべてのインターフェイスでのメール配信を有効にします。

C. CLI コマンド alt-src-host を使用して、新しいインターフェイスを配信候補として設定します。

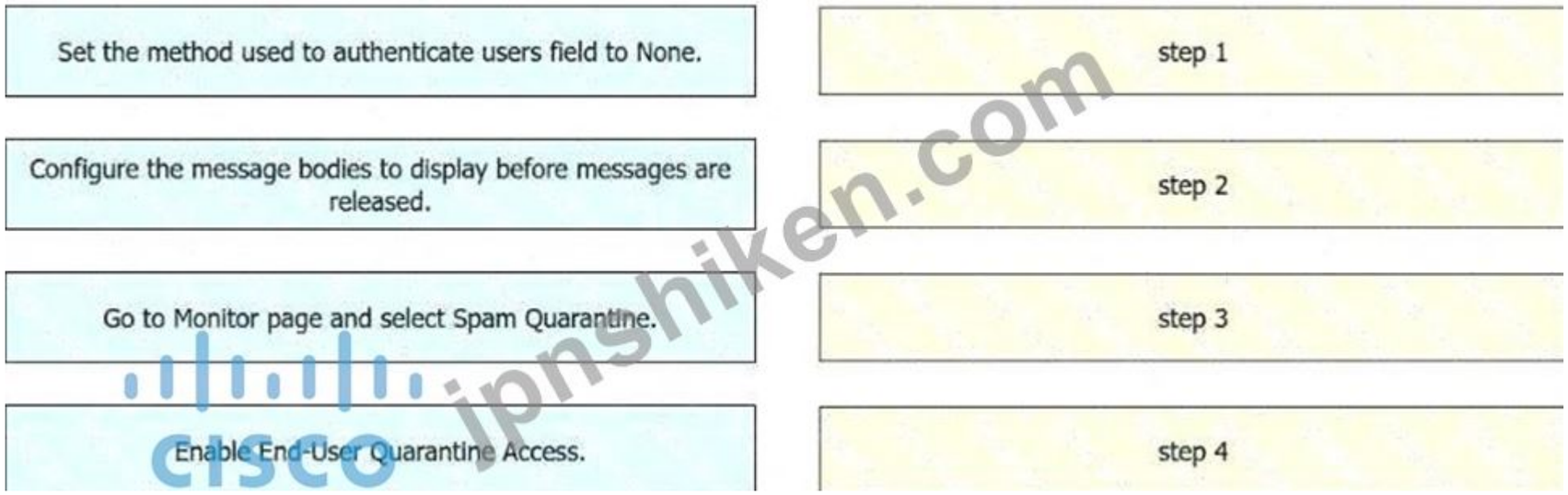
D. CLI コマンドdeliveryconfig を使用して、新しいインターフェイスをメール配信のプライマリ インターフェイスとして設定します。

正解: **D** (コメントを発表する)

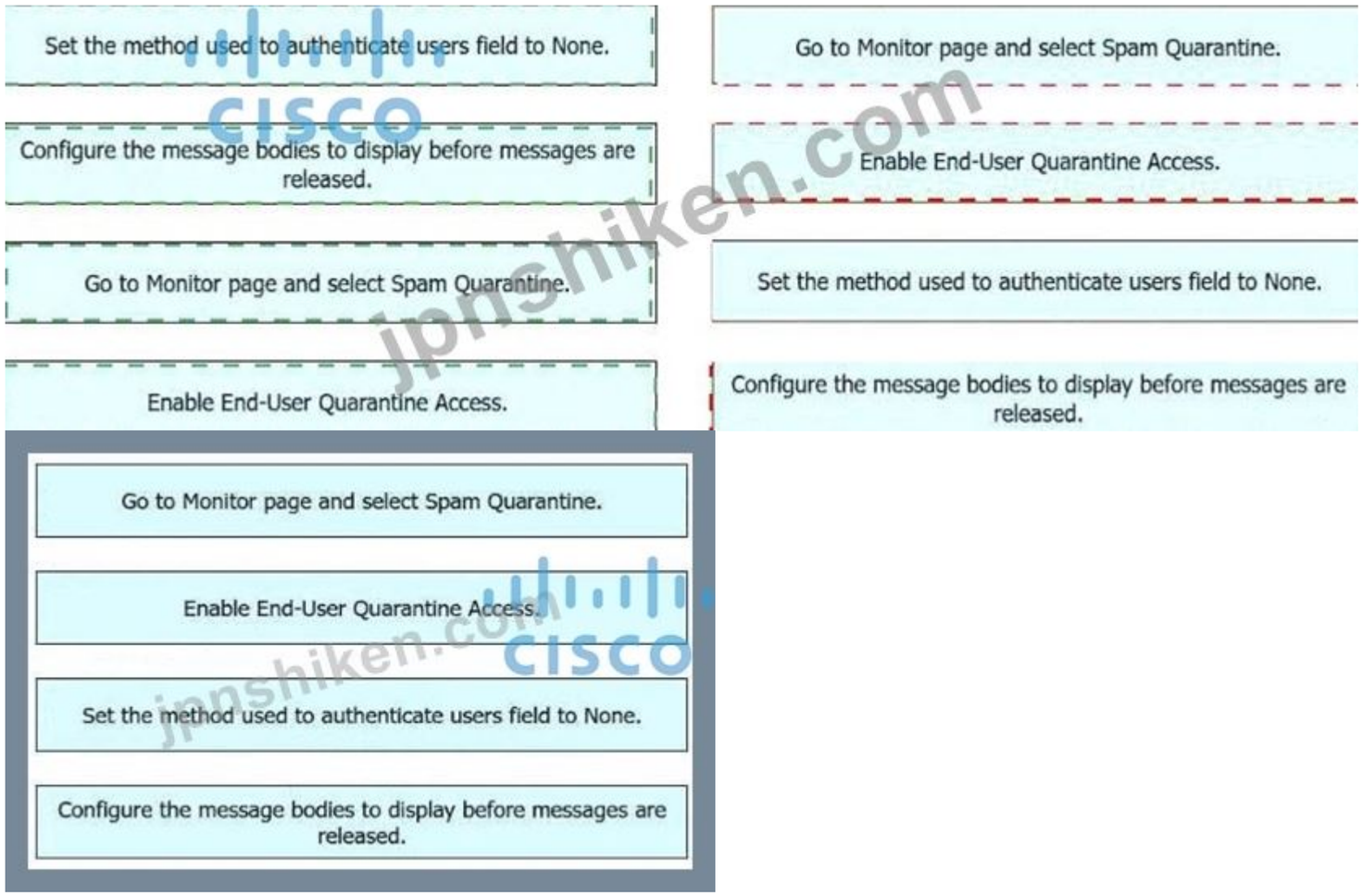
Determining Which Interface is Used for Mail Delivery Unless you specify the output interface via the deliveryconfig < /code > command or via a message filter (alt-src-host), or through the use of a virtual gateway, the output interface is selected by the AsyncOS routing table. https://www.cisco.com/c/en/us/td/docs /security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_0110 01.html? bookSearch=true

質問: **16**

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。



正解:

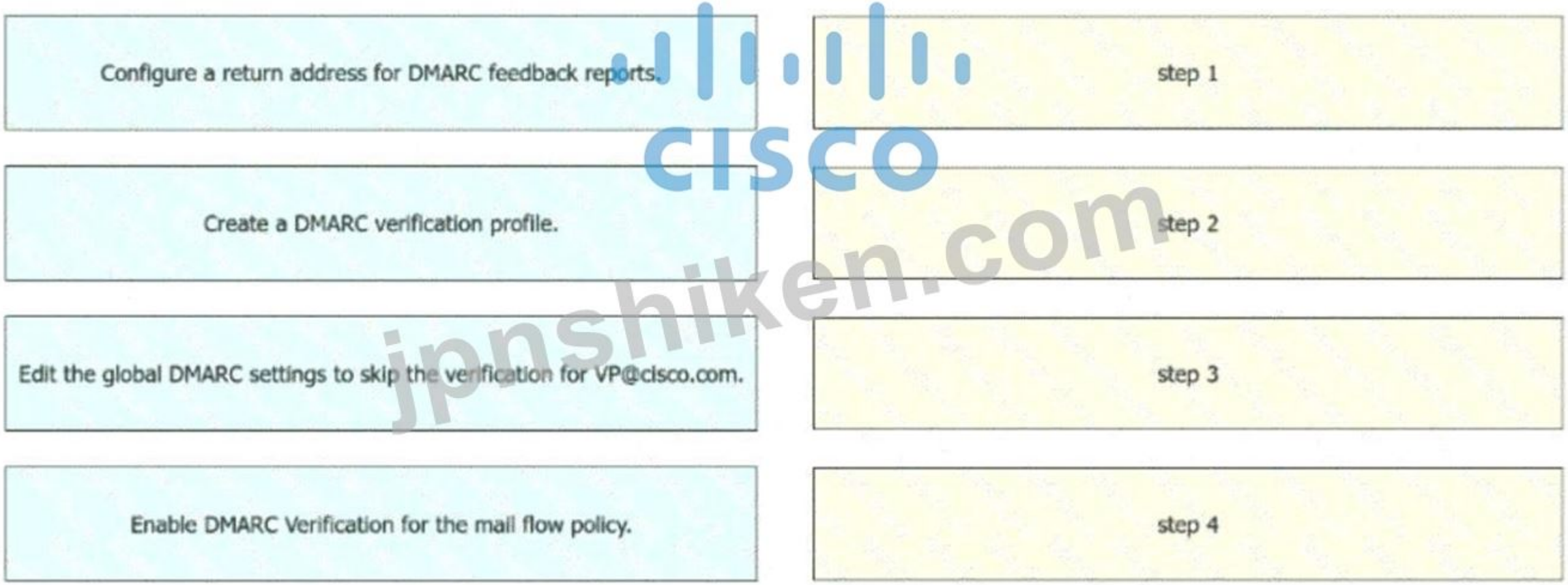


有効的な**300-720J**問題集はJPNTest.com提供され、**300-720J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-720J**試験問題集を提供します。JPNTest.com 300-720J試験問題集はもう更新されました。ここで**300-720J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-720J-mondaishu　**244**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」

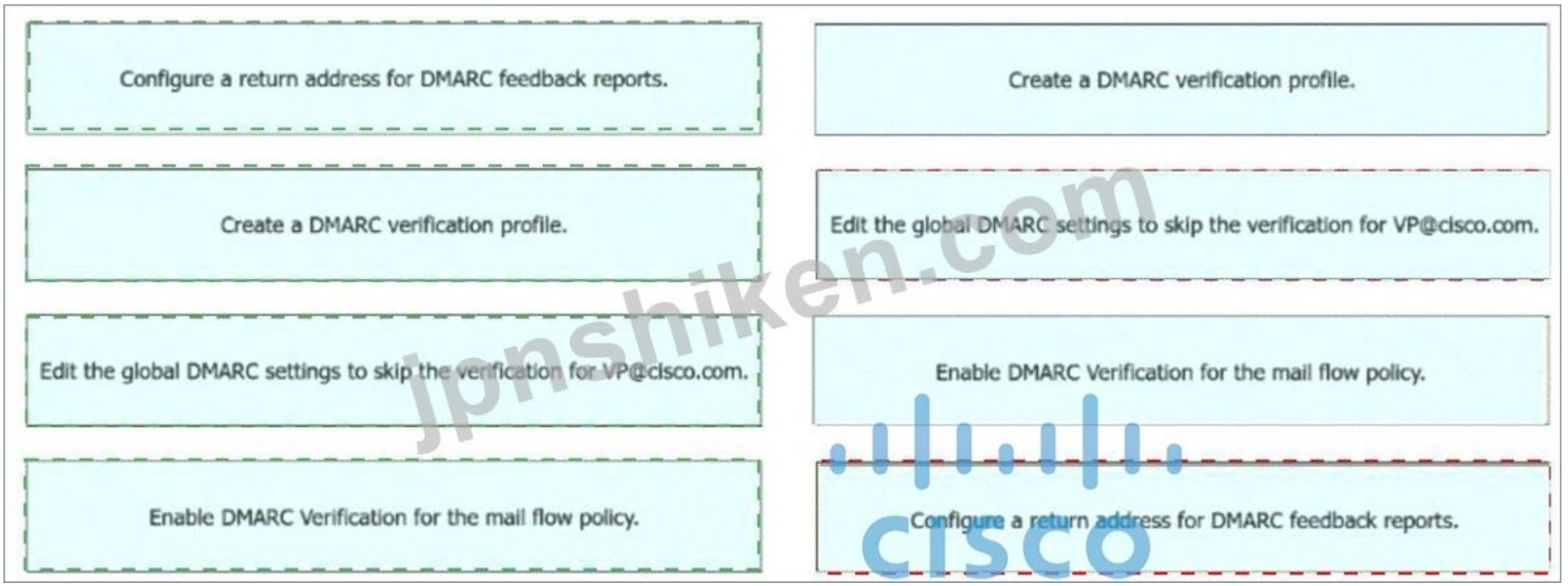
質問: **17**
一元化されたスパム検疫を使用してCisco ESAからCisco SMAに電子メールを配信するデフォルトのポートは何ですか？
A. 8025
B. 6443
C. 6025
D. 8443
正解: **C** (コメントを発表する)
The default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine is 6025. This is the default value for the Port setting in the External Spam Quarantine configuration on Cisco ESA. This port must be open on both Cisco ESA and Cisco SMA for the communication to work.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-4.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure- esa-00.html

質問: **18**
Cisco Secure Email Gateway 管理者は最近、アウトブレイク フィルタのグローバル サービス設定を有効にして、ウイルスと非ウイルスの脅威の検出を検出しましたが、アウトブレイク フィルタを 24 時間監視しても非ウイルスの脅威は検出されませんでした。非ウイルスの脅威が検出される理由は何ですか検出では肯定的な判定が検出されませんか?
A. 非ウイルス脅威の検出が適切に機能するには、ウイルス対策または AMP の有効化が必要です
B. アウトブレイク フィルター オプションのグレイメール ヘッダーを有効にする必要があります
C. 非ウイルス脅威の検出が適切に機能するには、アンチスパムまたはインテリジェント マルチスキャンの有効化が必要です。
D. アウトブレイク フィルター オプションの URL 書き換えを有効にする必要があります。
正解: **C (**コメントを発表する**)**
According to the [Cisco Secure Email User Guide], Non-Viral threat detection is a feature of Outbreak Filters that detects a nd blocks email messages that contain non-viral threats such as phishing, fraud, or social engineering[1 , p. 25]. To use this feature, you need to enable either AntiSpam or Intelligent Multi-Scan on your Cisco Secure Email Gateway, as these features provid e the necessary scanning and filtering capabilities for Non-Viral threat detection[1 , p. 26].
The other options are not valid because:
* A. Non-Viral threat detection does not require Antivirus or AMP enablement to properly function.
Antivirus and AMP are features that detect and block email messages that contain viral threats such as malware or ransomware[1 , p. 27-28].
* B. The Outbreak Filters option Graymail Header does not affect Non-Viral threat detection. Graymail Header is an option that allows you to add a header to email messages that are classified as graymail, which are messages that are not spam but may be unwanted by some recipients, such as newsletters or promotions[1 , p. 25].
* D. The Outbreak Filters option URL Rewriting does not affect Non-Viral threat detection. URL Rewriting is an option that allows you to rewrite the URLs in email messages to point to a Cisco proxy server, which can scan the URLs for malicious content and redirect the users to a warning page if needed[1 , p. 25].

質問: **19**
エンジニアは、Cisco Secure Email Gateway において、DM ARC を使用して受信メッセージの検証を設定する必要があります。



正解:



Explanation:

Create a DMARC verification profile.
Edit the global DMARC settings to bypass DMARC for VP@cisco.com
Enable DMARC Verification for the mail flow policy (select the profile).
Configure a return address for DMARC feedback reports.

質問: **20**
Cisco Secure Email Gateway で SMTP 認証中に CRL をチェックする目的は何ですか?
A. 日付を検証して証明書がまだ有効かどうかを確認します。
B. 証明書が失効していないか確認してください。
C. 該当するCAが存在することを確認
D. 共通名がユーザー ID と一致することを確認します。
正解: **B (**コメントを発表する**)**
The purpose of checking the Certificate Revocation List (CRL) during SMTP authentication on a Cisco Secure Email Gateway is to check if the certificate is not revoked by the issuing Certificate Authority (CA). A revoked certificate means that it is no longer valid and should not be trusted. References = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring SMTP Authentication [Cisco Secure Email Gateway] - Cisco]

質問: **21**
後方散乱に対抗するには、Cisco Secure Email Gateway でどの機能をアクティブにする必要がありますか?
A. グレイメールの検出
B. バウンス検証
C. 偽造メールの検出
D. バウンスプロファイル
正解: **(**正解を表示します**)**
To combat backscatter, which is a type of spam that consists of bounce messages sent to forged sender addresses, the administrator must enable the Bounce Verification feature under Security Settings. This feature allows the appliance to verify whether a bounce message is legitimate or not by checking if the original message was sent from the appliance. If not, the bounce message is considered as backscatter and can be dropped or quarantined. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Bounce Verification]

質問: **22**
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.: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-5.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/ b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011111.html

質問: **23**
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: **C** (コメントを発表する)
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118136-qanda-esa-00.html
You can use the SMTP route feature on Cisco ESA to specify how messages for a specific domain are routed to their destination. You can modify the SMTP route for the domain abc.com and change the IP address to
192.168.1.10 to ensure that messages a re delivered correctly 3 . References = Securing Email with Cisco Email Security Appliance (SESA) v3.1

質問: **24**
ある企業のCFOが、特定のヨガスタジオの週刊ニュースレターからのグレーメールを例外として設定するようメール管理者に依頼しています。これはどの種類のグレーメールに該当しますか？
A. 売上
B. 質量
C. マーケティング
D. ソーシャルネットワーク
正解: (正解を表示します)

質問: **25**
Cisco Secure Email Encryption Service の大きな添付ファイル（25MB を超える）機能に関して正しいのは、次の 2 つの記述のうちどれですか? (2つお選びください。)
A. 大きな添付ファイルは、Websafe ポータルを使用してのみ送信できます。
B. この機能を使用すると、ユーザーは安全な電子メールで最大 50MB の添付ファイルを送信できます。
C. 大きな添付ファイルは securedoc 添付ファイルとして送信されます。
D. 大きな添付ファイルは、Cisco Secure Email アドインを使用してのみ送信できます。
E. この機能は、メッセージからの読み取り機能が有効になっている場合にのみ有効になります。
正解: (正解を表示します)
* Large file attachments will be sent as a securedoc attachment. This means that the recipient will receive an encrypted message with a securedoc.html attachment that contains a link to download the large file from the Cisco Secure Email Encryption Service portal[2 , p. 9].
* This feature can only be enabled if the Read from Message feature is enabled. The Read from Message feature allows you to encrypt messages based on keywords or phrases in the subject or body of the me ssage. You need to enable this feature before you can enable the large file attachments feature[2 , p. 8].
The other options are not valid because:
* A. Large file attachments can be sent using both the websafe portal and the Cisco Secure Email Add-In.
The we bsafe portal allows you to compose and send encrypted messages from any web browser, while the Cisco Secure Email Add-In allows you to encrypt messages from your email client such as Outlook[
2 , p. 6-7].
* B. This feature allows users to send up to 100MB of a ttachments in a secure email, not 50MB[2 , p. 9].
* D. Large file attachments can be sent using both the websafe portal and the Cisco Secure Email Add-In.

The websafe portal allows you to compose and send encrypted messages from any web browser, while the Cis co Secure Email Add-In allows you to encrypt messages from your email client such as Outlook
[2 , p. 6-7].

質問: **26**
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**)**
Configuring DomainKeys and DKIM Signing:
-Signing Keys
-Public Keys
-Domain Profiles
Creating Domain Profiles:
Step 1
-Choose Mail Policies > Signing Profiles.
Step 2
-In the Domain Signing Profiles section, click Add Profile.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_1 4-0
/b_ESA_Admin_Guide_12_1_chapter_010110.html?bookSearch=true

質問: **27**
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 policie s to them based on their LDAP attributes[4 , p. 2].
* 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 crit eria and perform actions such as quarantine, encrypt, or drop the message[4 , p. 7].
The other options are not valid because:
* C. Uploa ding a csv file containing the email addresses for the users for whom you want to create mail policies is not a supported feature of Cisco Secure Email 1 .
* D. Enabling the content-scanning features you want to use with mail policies is not necessary, as content scanning is enabled by default for all incoming and outgoing messages[4 , p.

6].
* E. Defining the default mail policies for incomin g or outgoing messages is not sufficient, as default mail policies apply to all users and do not allow for differentiation based on user groups[4 , p. 2].

質問: **28**
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. ファイル評価フィルタリング
B. コンテンツフィルタ設定
C. ファイル分析
D. メッセージフィルター
E. 不適切なURL設定
正解: **(**正解を表示します**)**

質問: **29**
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. 非最終アクション
B. フィルター操作
C. アクションを破棄
D. 最終アクション
E. 検疫アクション
正解: **(**正解を表示します**)**
Non-final actions are actions that do not terminate the message filter evaluation, such as adding headers, setting variables, logging, etc. Final actions are actions that end the message filter evaluation and determine the fate of the message, such as accept, drop, bounce, quarantine, etc.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 3-4.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/ b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01000.html

質問: **30**
ネットワーク管理者は、Cisco Secure Email Gateway で McAfee ウイルス対策スキャンを有効にし、ウイルス スキャン アクションを 「ウイルスのみスキャン」に設定しました。スキャナが受信電子メールの添付ファイルにウイルスを検出した場合、このメッセージにはどのようなアクションが適用されますか?
A. 電子メールと添付ファイルはネットワーク管理者に転送されます。
B. 修復は試行されず、添付ファイルは落下または配送されました。
C. 添付ファイルは削除され、「削除された添付ファイル」ファイルに置き換えられます。
D. システムはアタッチメントの修復を試みます。
正解: **B (**コメントを発表する**)**
If the McAfee antivirus scanning is enabled on the Cisco Secure Email Gateway and the virus scanning action is set to "scan for viruses only", then no repair is attempted, and the attachment is either dropped or delivered based on the antiv irus policy settings. The administrator can choose to drop or deliver the infected attachment by selecting the appropriate action in the antivirus policy. References : [Cisco Secure Email Gateway Administrator Guide - Configuring McAfee Antivirus Scanning]

質問: **31**

URLを含む電子メールは、すべてのメールポリシーでコンテンツフィルタリングが無効になっているCiscoESAを通過します。送信者はsampleuser@test1.com、受信者はtestuser1 @ test2.com、testuser2 @ test2.com、testuser3 @ test2.com、mailer1 @ test2.comです。電子メールの件名はテストドキュメント395898847です。管理者は、この電子メールを許可する前に、CiscoESAがWebレピュテーションスコアを評価することを保証するポリシーを追加したいと考えています。
これを達成するために管理者が使用する必要がある2つの基準はどれですか？　2つ選択してください。）
A. Subject contains Test Document"
B. Sender matches test1.com
C. Email body contains a URL
D. Date and time of email
E. Email does not match mailer1@test2.com
正解**: B,C (**コメントを発表する**)**
Web reputation score is a feature that allows Cisco ESA to evaluate the reputation of URLs in messages based on real-time data from Talos intelligence and apply appropriate actions, such as block, quarantine, or deliver.
To ensure that Cisco ESA evaluates the web reputation score before permitting this email, the administrator should use two criteria to create a content filter or message filter that matches this email and applies an action of "check web reputation":
* Sender matches test1.com, which means that the sender's domain name is test1.com.
* Email body contains a URL, which means that the message body has one or more URLs in it.
The other options are not valid criteria to ensure that Cisco ESA evaluates the web reputation score before permitting this email, because they do not match this email or they are not relevant to web reputation score.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , pag e 8-3 and page 8-7.

有効的な**300-720J**問題集はJPNTest.com提供され、**300-720J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-720J**試験問題集を提供します。JPNTest.com 300-720J試験問題集はもう更新されました。ここで**300-720J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-720J-mondaishu　**244**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」

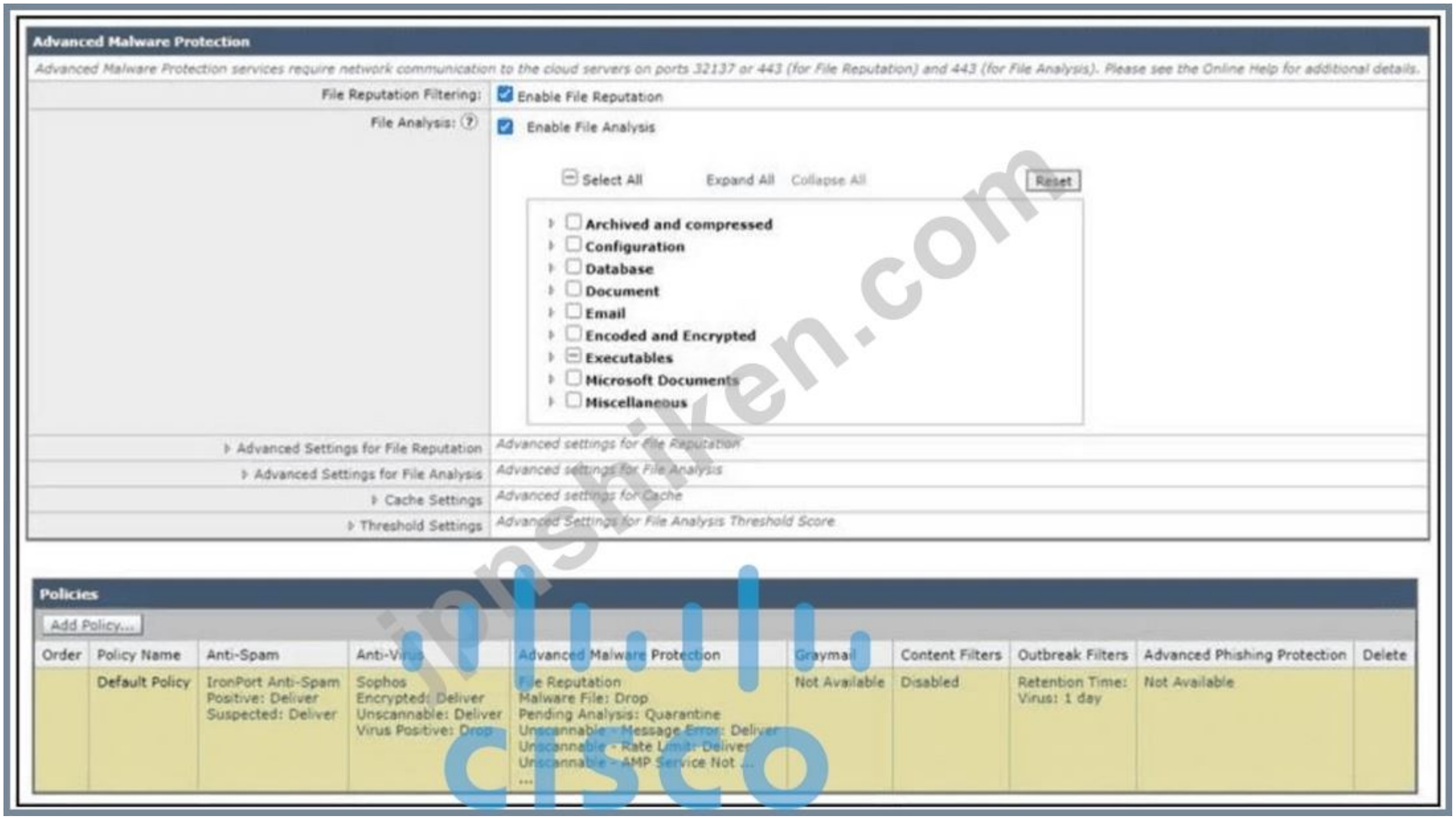
質問**: 32**
メール管理者は、Cisco Secure Email Gateway 上で DLP ポリシーを設定する必要があります。DLP ポリシーは、デフォルトの送信メール ポリシーに追加する必要があります。この作業はどのように行うのでしょうか？
A. DLP評価ウィザードを活用する前に、同じ重大度レベルのDLPポリシーを削除してください。
B. DLP評価ウィザードを使用する前に、既存のDLPポリシーをすべて削除してください。
C. 定義済みのDLPポリシーテンプレート内の特定のコンテンツに一致する分類子を作成します。
D. DLP ポリシーの受信者グループを作成し、それを既定の送信メール ポリシーに適用します。
正解**: (**正解を表示します**)**
質問**: 33**

```
TEST: if (forged-email-detection ("support", 60)) { fed("from", ""); }
```

図を参照してください。エンジニアは、既存の偽造メール検出メッセージフィルタを変更して、 Executives」という名前の新しく作成された辞書を参照するようにする必要があります。この課題を達成するには、何をすべきでしょうか？
A. Change " from " to " Executives " .
B. Change " TESF to " Executives " .

C. Change fed ' to " Executives " .
D. Change " support " to " Executives " .
正解: (正解を表示します)
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKSEC-2240.pdf

質問: **34**



図を参照してください。Cisco Secure Email Gatewayは、未知のMicrosoft Word文書が添付されたメールをどのように処理しますか？
A. メールはファイル解析なしで配信されます。
B. メールは隔離されています。
C. ファイルはファイル分析のためにクラウドに送信されます。
D. メールは破棄されました。
正解: (正解を表示します)

質問: **35**

```
Tue Aug 13 16:55:40 2019 Info: Start MID 379133 ICID 391963
Tue Aug 13 16:55:40 2019 Info: MID 379133 ICID 391963 From: <matt@lee.com>
Tue Aug 13 16:55:40 2019 Info: MID 379133 ICID 391963 RID o To: <bob_doe@cisco.com>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Message-ID '<op.z6f21uf7uxysu20mathuynh-f645d.mshome.net>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Subject 'This is a highly confidential email.'
Tue Aug 13 16:55:48 2019 Info: MID 379133 ready 12142757 bytes from <matt@lee.com>
Tue Aug 13 16:55:49 2019 Info: MID 379133 matched all recipients for pre-recipient policy marketing team in the inbound table
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/524208) for scanning by Outbreak Filters
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/2097152) for scanning by CASE
Tue Aug 13 16:55:50 2019 Info: MID 379133 interim AV verdict using Sophos CLEAN
Tue Aug 13 16:55:50 2019 Info: MID 379133 antivirus negative
Tue Aug 13 16:55:50 2019 Info: MID 379133 using engine: GRAYMAIL negative
Tue Aug 13 16:55:52 2019 Info: MID 379133 attachment 'ds_validation_NEG.zip'
Tue Aug 13 16:55:52 2019 Warning: MID 379133, Message Scanning Problem: Size Limit Exceeded
Tue Aug 13 16:55:52 2019 Info: MID 379133 queued for delivery
```

Scan Behavior

Attachment Type Mappings

Add Mapping...

Fingerprint/MIME	Type	Edit	Delete
Fingerprint	Image	Edit...	
Fingerprint	Media	Edit...	
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	

Export List...

jpnshiken.com
CISCO

Global Settings	
Action for attachments with MIME types/fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled
	Edit Global Settings...

cisco
jpnshiken.com

図を参照してください。Cisco ESAで添付ファイルをスキャンできるようにするには、スキャン動作のどの設定を更新する必要がありますか？

A. zip ファイルの添付ファイルタイプにマッピングを追加します。

B. 何らかの理由でメールがスキャンされなかった場合に、一致するパターンを想定することを有効にします。

C. 最大再帰深度を 5 からより大きな値に増やします。

D. スキャンする添付ファイルの最大サイズをより大きな値に増やします。

正解: **D** (コメントを発表する)

The maximum attachment size to scan is a configuration on the scan behavior that determines the maximum size of an attachment that Cisco ESA will scan for viruses and malware. If an attachment exceeds this size, Cisco ESA will apply the configured action for unscannable messages, such as deliver, drop, or quarantine.

To allow the attachment to be scanned on the Cisco ESA, this configuration must be updated to a larger value than the attachment size, which is 10 MB according to the message header.

The other options are not valid configurations to allow the attachment to be scanned on the Cisco ESA, because they do not affect the maximum attachment size to scan.

References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 7-3 and page 7-4.

質問: **36**

ある組織は、企業ポリシーによりエンドユーザーによる隔離への直接アクセスが許可されていないため、スパム隔離からのメッセージの解放を要求するチケットを支援するヘルプ デスク担当者を指名したいと考えています。Cisco Secure Email Gateway で設定を変更するためのアクセスを制限しながら、ヘルプ デスク担当者がメッセージをリリースできるようにするには、次の 2 つの役割を使用する必要がありますか? (2つお選びください。)

A. 管理者

B. ヘルプデスクユーザー

C. 読み取り専用演算子

D. 技術者

E. 隔離管理者

正解**: B,E (**コメントを発表する**)**

All users with administrator privileges can change spam quarantine settings and view and manage messages in the spam quarantine. You do not need to configure spam quarantine access for administrator users.

If you configure access to the spam quarantine for users with the following roles, they can view, release, and delete messages in the spam quarantine:

-Operator

-Read-only operator

-Help desk user

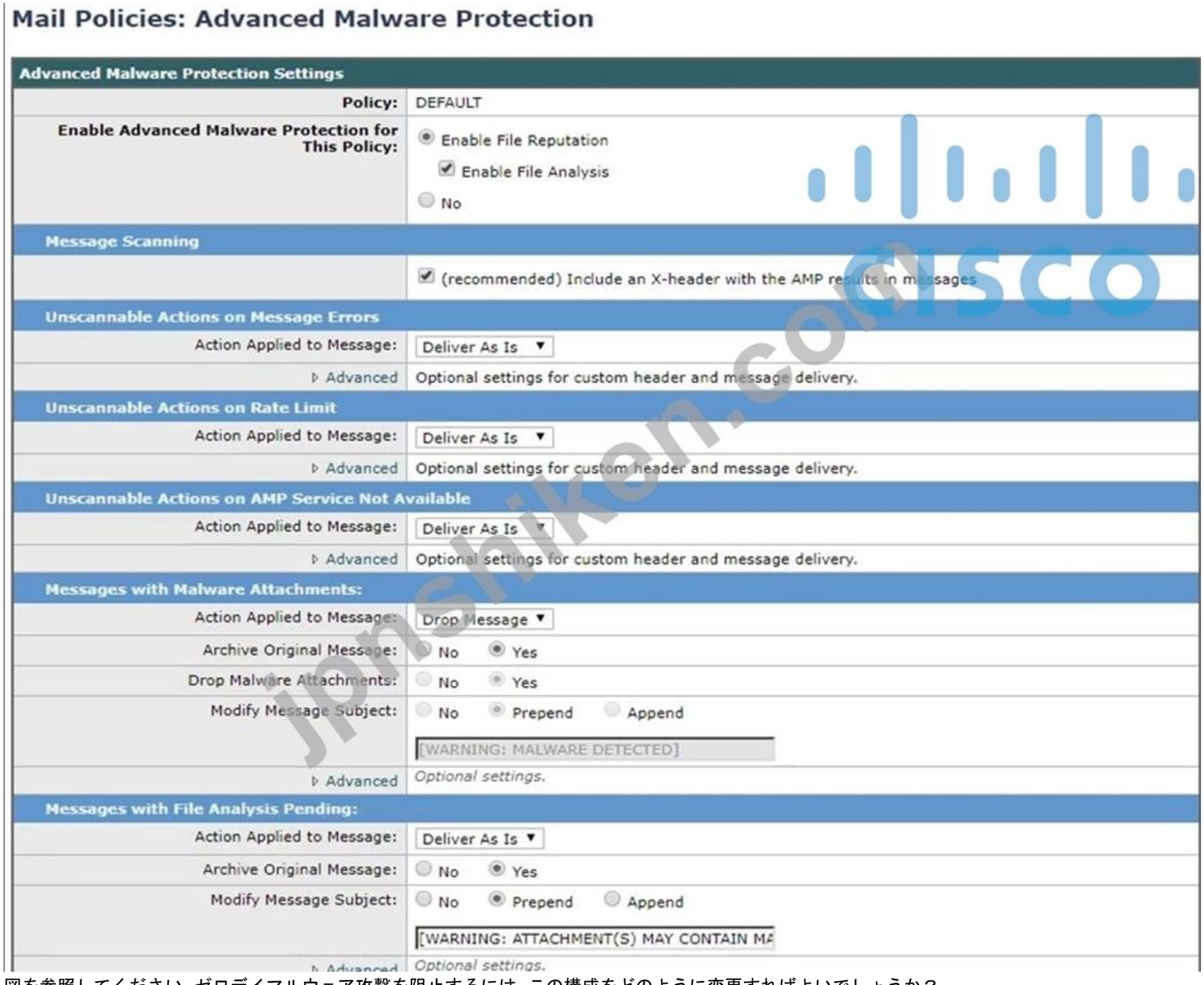
-Guest

-Custom user roles that have spam quarantine privileges

These users cannot access spam quarantine settings.

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**: 37**



図を参照してください。ゼロデイマルウェア攻撃を阻止するには、この構成をどのように変更すればよいでしょうか？

A. 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。

B. 変更ファイル分析保留中のアクションは 現状のまま納品」から 隔離」に変更されます。

C. メールボックスの自動修復を設定します。

D. マルウェア添付ファイルの下にあるメッセージ件名の変更にプレフィックスを適用します。

正解: (正解を表示します)
Overview of File Reputation Filtering and File Analysis:
Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:
-Obtaining the reputation of known files.
-Analyzing behavior of certain files that are not yet known to the reputation service.
-Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.
-This feature is available for incoming messages and outgoing messages.
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_010000.html?bookSearch=true

質問: **38**
Cisco Secure Email Gateway アプライアンスは、無効な受信者の検証に送信された多くのメッセージを処理しています。このタスクを達成するために必要な 2 つの手順はどれですか? (2 つお選びください。)
A. 外部 LDAP 認証を有効にする
B. リスナーで LDAP クエリを構成します。
C. LDAP サーバー プロファイルを構成する
D. リスナーで LDAP 認証を有効にする
E. LDAP サーバーにクエリを実行するように受信メール ポリシーを構成します。
正解: (正解を表示します)
To enable LDAP recipient verification on a Cisco Secure Email Gateway appliance, you need to configure the LDAP query on a listener and configure LDAP server profiles. The LDAP query specifies the criteria for matching recipient addresses against an LDAP directory. The LDAP server profile defines the connection settings and authentication credentials for accessing an L DAP server 2 . References = User Guide for AsyncOS 12.0 for Cisco Email Sec urity Appliances - GD (General Deployment) - Configuring LDAP Queries [Cisco Secure Email Gateway] - Cisco

質問: **39**
スパマーは日常的に、受信者フィールドに文字と数字の可能なすべての組み合わせのリストを入力して電子メールを送信しようとします。会社のドメイン名が付加されたこれらの組み合わせは、考えられるすべての有効な電子メール アドレスを学習しようとする悪意のある試みです。この問題の発生を防ぐには、Cisco Secure Email Gateway でどのアクションを実行する必要がありますか?
A. [SMTP 認証クエリ] チェックボックスを選択します。
B. LDAP 受け入れ検証を実行します。
C. 外部認証クエリを隔離します。
D. エンド ユーザー セーフリスト機能を有効にする
正解: (正解を表示します)
LDAP acceptance validation is a feature that allows the Cisco Secure Email Gateway to check if the recipient address of an incoming message exists in an LDAP directory before accepti ng it. This feature can help prevent spammers from sending emails with invalid recipient addresses and reduce the load on the applia nce
2 . References = User Guide for AsyncOS 12.0 for Cisco Email Security A ppliances - GD (General Deployment) - Configuring LDAP Queries [Cisco Secure Email Gateway] - Cisco

質問: **40**
ある企業は、営業部門から外部に送信されるすべての電子メールを DLP でスキャンして PCI-DSS に準拠することを義務付ける新しい義務を導入しました。新しい DLP ポリシーが Cisco ESA 上に作成されており、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。

このタスクを達成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. 暫定的なメールポリシー
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**: (**正解を表示します**)**
Outgoing Mail Policy is a mail policy that should be created to accomplish this task. Outgoing Mail Policy is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.
To create an Outgoing Mail Policy named 'Sales' and assign a DLP policy to it, the administrator can follow these steps:
* Select Mail Policies > Outgoing Mail Policies and click Add Policy.
* Enter 'Sales' as the policy name and click Submit.
* Select 'Sales' from the list of policies and click Edit Settings.
* Under Data Loss Prevention, select Enable Data Loss Prevention Scanning and choose the DLP policy from the drop-down menu.
* Click Submit.
The other options are not valid mail policies to accomplish this task, because they do not apply to outgoing messages or DLP scanning.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway, page 9-2 and page 9-4.

質問**: 41**
エンジニアは、Cisco Secure Email Gateway で SMTP のディレクトリ ハーベスト攻撃防止を設定する必要があります。
このエラーメッセージは、リスナーが1時間に50件を超える無効な受信者を受信した場合に送信する必要があります。
*500 - リクエストが多すぎます
*1時間あたりの最大無効受信者数は既に50に設定されています。
要件を満たすために、1時間あたりの最大無効受信者数を設定するには、次にどの2つの操作を行う必要がありますか？
(2つ選択してください。)
A. 1時間あたりの最大受信者コードを500に作成します。
B. 1 時間あたりの最大受信者数テキストを 500 に適用します - リクエストが多すぎます。
C. 1時間あたりの最大受信者数を500に設定します。
D. 1 時間あたりの最大受信者数をテキスト 『リクエストが多すぎます」に設定します。
E. 1 時間あたりの最大受信者数を 500 にテキスト送信します - リクエストが多すぎます。
正解**: (**正解を表示します**)**

質問**: 42**
エンジニアは、クレジット カード番号を含む添付ファイルを検出し、さらなる措置が取られるまでレビューのために保存するコンテンツ フィルターを作成するという任務を負っています。この要件を満たすように Cisco Secure Email Gateway のどのコンポーネントを設定する必要がありますか?
A. スパム検疫
B. ポリシー隔離
C. アウトブレイクフィルター
D. コンテンツフィルター
正解**: D (**コメントを発表する**)**
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. References = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (Gene ral Deployment) - Content Filters [Cisco Secure Email Gateway] - Cisco]

質問: **43**
Cisco ESA電子メールパイプラインの2つのフェーズは何ですか？ (2つ選択してください。)
A. reject
B. workqueue
C. action
D. delivery
E. quarantine
正解: (正解を表示します)
With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography.
Configuring DomainKeys and DKIM Signing A signing key i s the private key stored on the appliance.
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?bookSearch=true
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-1/user_guide/ b_ESA_Admin_Guide_12_1/b_ESA_Admin_Guide_12_1_chapter_011.pdf (p.1)

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. [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。
B. 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。
C. 宛先コントロールを変更し、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。
D. [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。
正解: (正解を表示します)

質問: **45**
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. 帽子
B. 土
C. ネズミ
D. バット
正解: (正解を表示します)

質問: **46**
展示を参照してください。



このフィルタ構成から何が起こるでしょうか?

A. アクションはメールのウイルス対策チェックをすべてスキップします。

B. 件名が FW: バウンス通知」のすべてのメールにアクションが適用されます。

C. アクションはメールのすべてのスパム対策チェックをスキップします。

D. アクションは test@cisco.com からのすべてのメールに適用されます。

正解: **A** (コメントを発表する)

有効的な**300-720J**問題集はJPNTest.com提供され、**300-720J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-720J**試験問題集を提供します。JPNTest.com 300-720J試験問題集はもう更新されました。ここで**300-720J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-720J-mondaishu **244**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**

コンテンツフィルターの機能とは何ですか？

A. スパム対策スキャンを実行する

B. メール件名に基づいてメッセージを確認する

C. メッセージフィルターの前にルールを適用する

D. 受信または送信メッセージをスキャンする

正解: (正解を表示します)

質問: **48**

会社の幹部のリストは日常的になりすましされており、会社は悪意のある電子メール攻撃の危険にさらされています。管理者は、幹部のメッセージが正当な送信アドレスから発信されていることを確認する必要があります。このタスクを達成するには、どの 2 つの手順を実行する必要がありますか? (2つお選びください。)

A. SPF 検出を使用して受信コンテンツ フィルターを作成します。

B. [セキュリティ設定] で偽造メール検出機能を有効にします。

C. メール ポリシーで DMARC 機能を有効にします。

D. 偽造メール検出条件を使用して受信コンテンツ フィルターを作成します。

E. スプーフィングされている名前のリストを含むコンテンツ辞書を作成します。

正解: (正解を表示します)

To ensure that executive messages are originating from legitimate sending addresses, the administrator must take two steps:

* Create an incoming content filter with the Forged Email Detection condition. This will allow the administrator to detect and block messages that have a forged "From: header" that

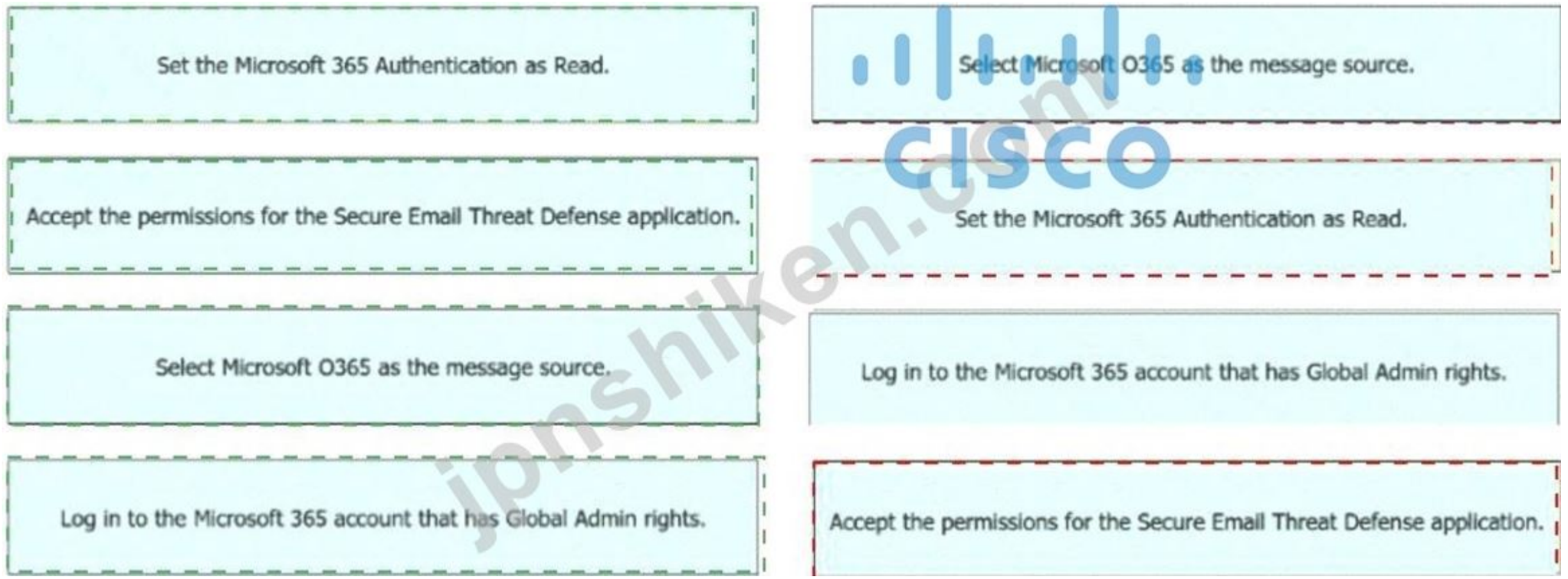
matches or is similar to any of the names in a content dictionary.
* Create a content dictionary including a list of the names that are being spoofed. This will allow t he administrator to specify the names of the executives that are being targeted by spoofing attacks and use them in the Forged Email Detection condition. The other options are not relevant or sufficient for this task. References : [Cisco Secure Email Gatewa y Administrator Guide - Forged Email Detection] and
[Cisco Secure Email Gateway Administrator Guide - Creating Content Dictionaries]

質問: **49**
Cisco Secure Email Threat DefenseをMicrosoft 365と統合する際には、エンジニアがメッセージソースを設定する必要があります。統合では、可視性は確保されますが、修復はできません。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。



jpnshiken.com
CISCO

正解:



Explanation:

Step 1: Select Microsoft O365 as the message source.

Step 2: Set the Microsoft 365 Authentication to Read (visibility only, no remediation).

Step 3: Log in with a Microsoft 365 Global Admin account.

Step 4: Accept the permissions requested for the Secure Email Threat Defense app.

質問: 50

展示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.

Therefore, the correct answer is C.

References:

SPF Record Syntax

Define your SPF record-Basic setup

質問: 51

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？

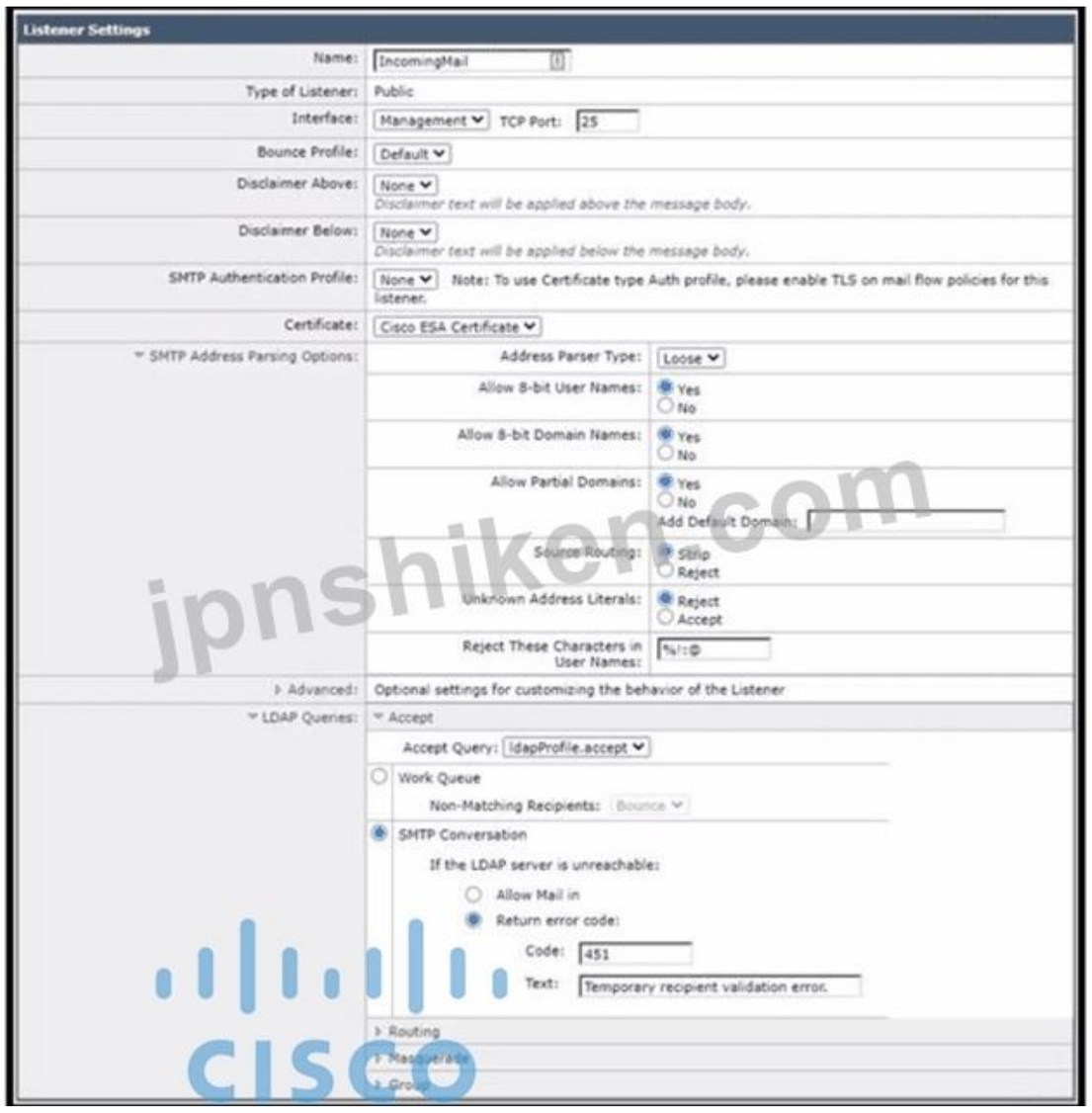
A. Talosをオーバーライドするメッセージフィルターを使用して、新しい受信メールポリシーを作成します。

B. 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。

C. 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。
D. ドメインを許可リストに追加します。
正解: **(**正解を表示します**)**
The allow list is a feature that allows Cisco ESA to accept messages from specific email addresses or domains, regardless of their sender-based reputation score or other reputation filters.
To allow inbound email from that specific domain, the administrator should add the domain into the allow list on Cisco ESA, which can be done from the web user interface by selecting Security Services > Safelist
/Blocklist and clicking Add Entry.
The other options are not valid solutions to allow inbound email from that specific domain, because they do not affect the sender-based reputation score or the reputation filters on Cisco ESA.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 6-13 and page 6-14.

質問: **52**
Cisco Secure Email Gateway をメッセージ ソースとして使用する場合にのみ使用できる Cisco Secure Email Threat Defense の可視性および修復モードはどれですか?
A. ベーシック認証
B. 認証なし
C. Microsoft 365 認証
D. Cisco セキュリティ クラウド サインオン
正解: **(**正解を表示します**)**
According to the Cisco Secure Email Threat Defense User Guide , the No Authentication option is only available if you are using a Cisco Secure Email Gateway (SEG) as your message source. This option allows visibility only, no remediation 1 .
The other options are not valid because:
* A. Basic Authentication is not a visibility and remediation mode for Cisco Secure Email Threat Defense. It is a method of authenticating users with a username and password 2 .
* C. Microsoft 365 Authen tication is a visibility and remediation mode that allows you to use Microsoft
365 credentials to access Cisco Secure Email Threat Defense. It has two sub-options: Read/Write and Read. This mode is available for both Microsoft 365 and Gateway message sources 1 .
* D. Cisco Security Cloud Sign On is not a visibility and remediation mode for Cisco Secure Email Threat Defense. It is a service that manages user authentication for Cisco security products, including Cisco Secure Email Threat Defense 3 .

質問: **53**
展示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には、どのような追加の構成アクションを実行す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 ハーベスト攻撃防御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構成します。

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構成します。

D. リスナー設定で、ワークキューを使用するように LDAP クエリ設定を変更します。

正解: **(**正解を表示します**)**

To protect against Directory Harvest Attacks, the administrator must configure D irectory 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 addresse s. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Directory Harvest Attack Prevention]

質問: **54**

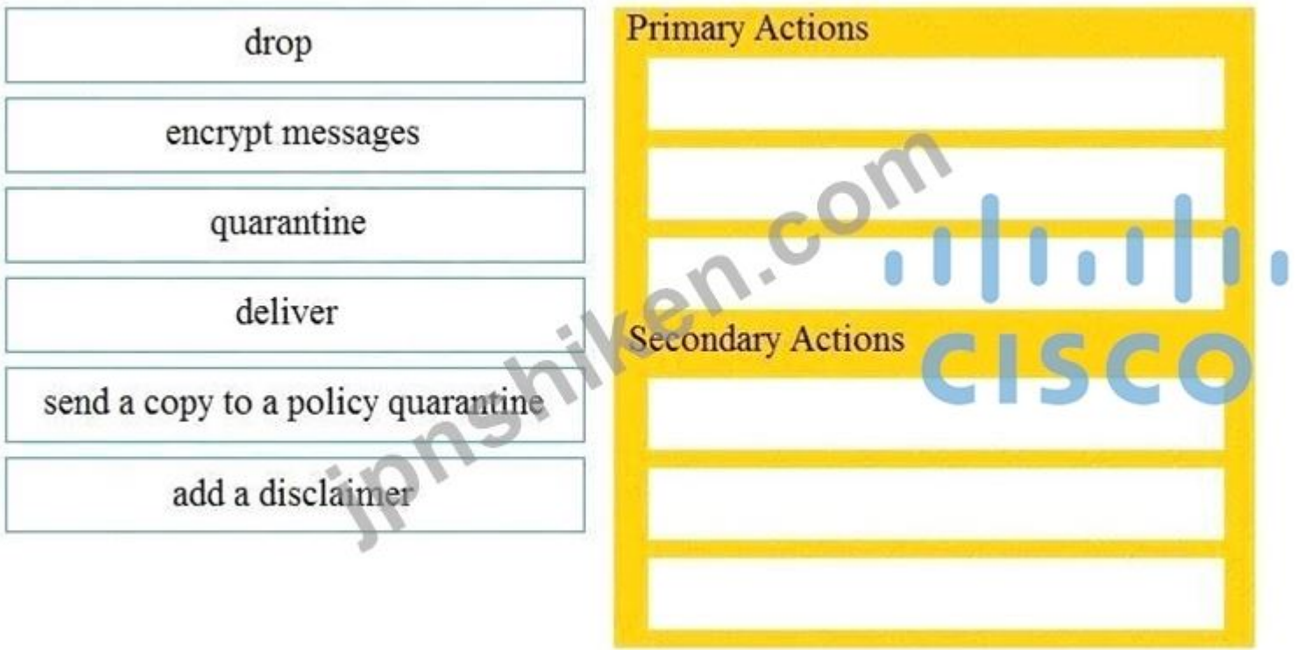
管理者が集中型PVOを有効にしようとしていますが、「クラスター内のesa1にはクラスターレベルとは異なるレベルで利用可能なコンテンツフィルター/ DLPアクションがあるため、集中型ポリシー、ウイルス、および大規模感染の隔離設定を続行できません。」というエラーを受け取ります。このエラーの原因は何ですか？

A. コンテンツフィルターは、esa1のマシンレベルで構成されます。

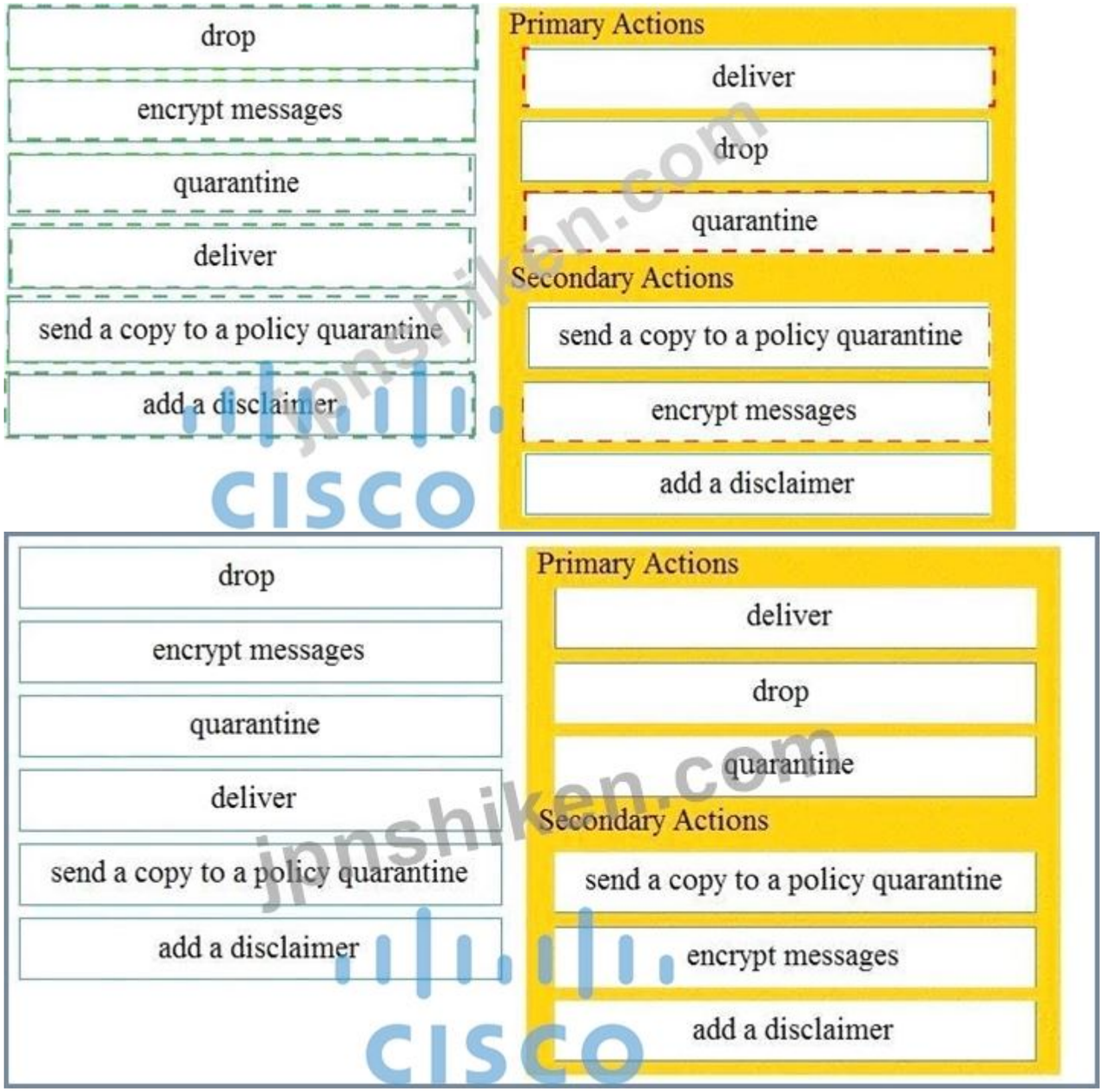
B. DLPはesa2のクラスターレベルで構成されます。
C. DLPはesa1のドメインレベルで構成されます。
D. DLPはhost1で構成されていません。
正解: (正解を表示します)
The PVO cannot be enabled and shows this type of error message.
Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines configuration as host1 and host2 in Cluster have content filters / DLP actions available at a level different from the cluster Level.
The error message can indicate that one of the hosts does not have a DLP feature key applied and DLP is disabled. The solution is to add the missing feature key and apply DLP settings identical as on the host that has the feature key applied. This feature key inconsistency might have the same effect with Outbreak Filters, Sophos Antivirus, and other feature keys.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote- esa-00.html

質問: **55**
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 という名前の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。テーブルに何を追加する必要がありますか？
A. NewInterface@cisco.com
Cisco、10.10.10.1
B. @cisco.com NewInterface
C. cisco.com NewInterface
正解: (正解を表示します)

質問: **56**
考えられる DLP に対する Cisco ESA の反応を左側から右側の正しいアクション タイプにドラッグ アンド ドロップします。



正解:



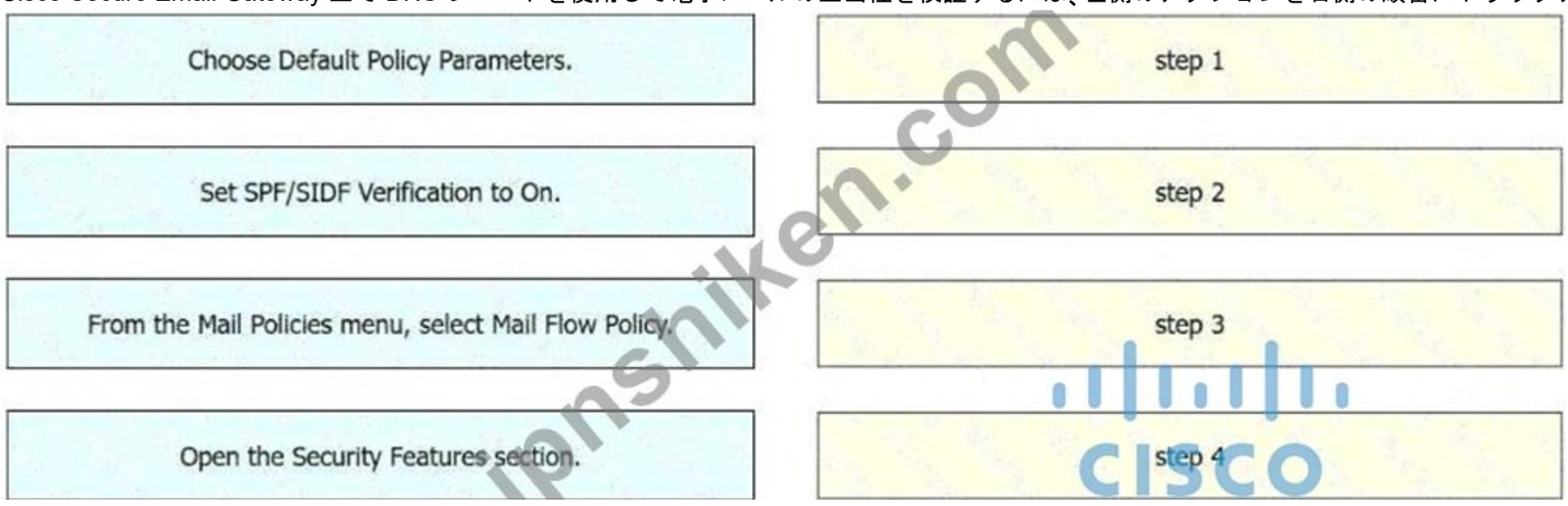
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/ b_ESA_Admin_Guide_chapter_010001.html (message actions)

質問: **57**
Cisco ESAでURLロギングが設定されている場合、どの機能を最初に有効にする必要がありますか？
A. ウイルス対策
B. スパム対策
C. ウイルス発生フィルター
D. senderbaseレピュテーションフィルター
正解: **(**正解を表示します**)**
Enabling Logging of URLs and Message Tracking Details for URLs

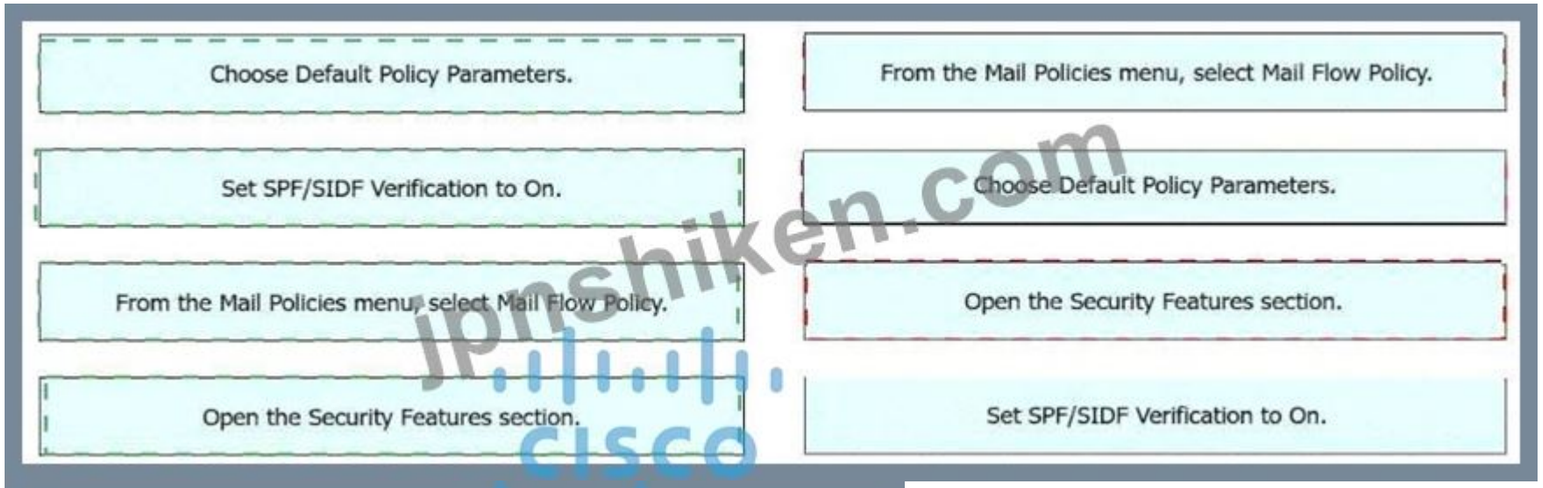
Logging of URL-related logs, and display of this information in Message Tracking details, is disabled by default. This includes the logs for the following events:
Category of any URL in the message matches the URL category filters
Reputation score of any URL in the message matches URL reputation filters Outbreak Filter rewrites any URL in the message To enable logging of these events, use the outbreakconfig command in the command-line interface (CLI).
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?bookSearch=true
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote- esa-00.html (note under enable url filtering)

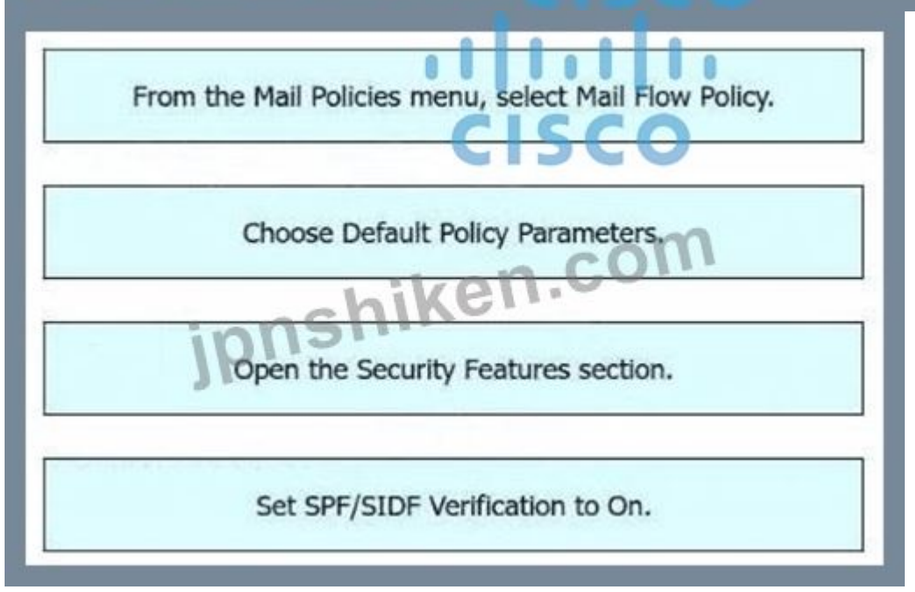
質問: **58**
DLPスキャンを実行するには、どの2つのコンポーネントを構成する必要がありますか？ （2つ選択してください。）
A. 受信メールポリシーにDLPポリシーを追加します。
B. DLPポリシーマネージャーにDLPポリシーを追加します。
C. 送信メールポリシーでDLPポリシーを有効にします。
D. DLPポリシーのカスタマイズでDLPポリシーを有効にします。
E. DLPポリシーを送信コンテンツフィルターに追加します。
正解: **(正解を表示します)**
To perform DLP scanning on Cisco ESA, two components must be configured:
* Add a DLP policy to the DLP Policy Manager, which is a repository of predefined or custom DLP policies that specify what types of data to scan for and what actions to take if a match is found.
* Enable a DLP policy on the Outgoing Mail Policy, which is a set of rules that determine how outgoing messages are processed by Cisco ESA, including whether to apply DLP scanning or not.
References: User Guide f or AsyncOS 15.0 for Cisco Secure Email Gateway , page 9-2 and page 9-4.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/ b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_010001.html

質問: **59**
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:





jpnshiken.com
cisco
cisco
jpnshiken.com

質問: **60**
Cisco Secure Email Gateway アプライアンスで Cisco SecureX 統合を有効にするには、次の 2 つの手順のうちどれが必要ですか? (2つお選びください。)
A. スマート ライセンス アカウントから生成された登録トークンを貼り付けます。
B. [ネットワーク] > [クラウド サービス設定] で Threat Response サービスを有効にします。
C. 地域に基づいて適切な Threat Response Server を選択します。
D. Security Services Exchange から生成された登録トークンを貼り付けます。
E. [ネットワーク] > [クラウド サービス設定] で Security Services Exchange サービスを有効にします。
正解: **(**正解を表示します**)**
one of the methods to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance is to use the Threat Response service 1 . This s ervice allows the appliance to send telemetry data to the SecureX cloud and provide visibility and response capabilities across multiple security products 1 . To use this service, the administrator needs to perform the following steps 1 :
* Enable the Threat Respons e service: The administrator needs to go to Network > Cloud Service Settings and enable the Threat Response service. This will generate a registration token that can be use d to register the appliance with SecureX 1 .
* Select the correct Threat Response Server: The administrator needs to select the appropriate Threat Response server based on the region where the appliance is located. The availa ble regions are North America, Europe, and Asia Pacific 1 .

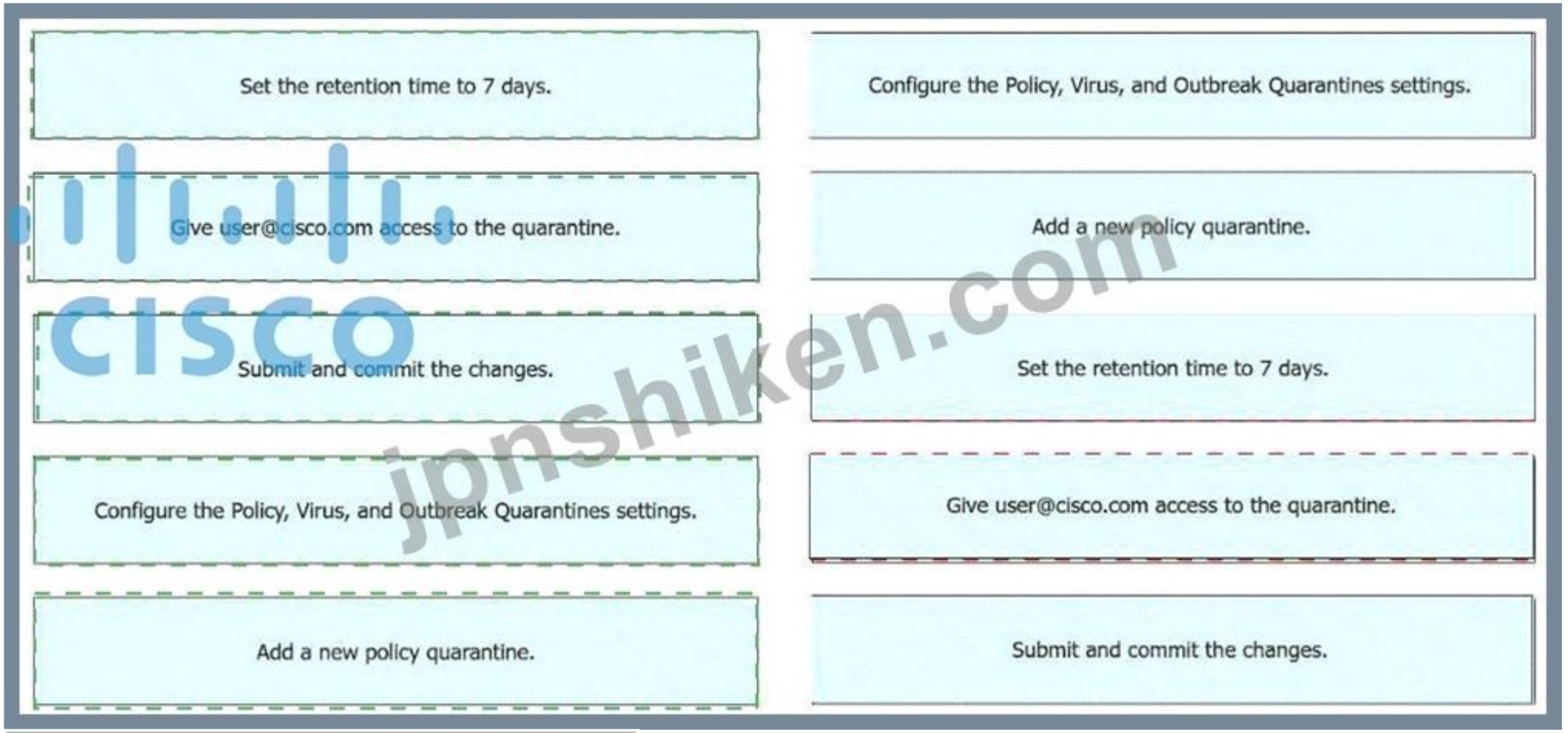
質問: **61**

エンジニアは、Cisco Secure Email Gatewayでポリシー隔離を設定する必要があります。保持期間は7日間とし、user@cisco.comが隔離領域にアクセス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のシーケンスにドラッグアンドドロップしてください。



正解:

jpnshiken.com



有効的な**300-720J**問題集はJPNTest.com提供され、**300-720J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-720J**試験問題集を提供します。JPNTest.com 300-720J試験問題集はもう更新されました。ここで**300-720J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-720J-mondaishu　**244**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
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: **(正解を表示します)**
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.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 5-14 and page 5-15.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118542-qa-esa- 00.
html

質問: **63**
展示を参照してください。



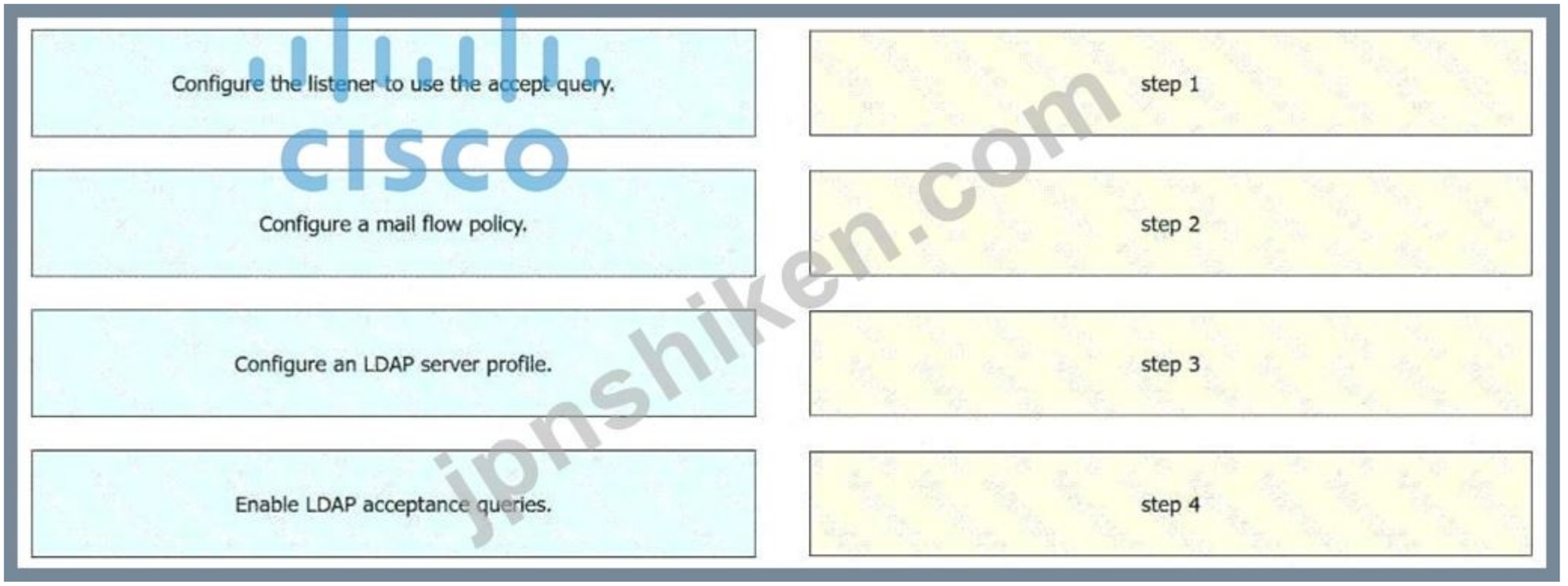
ネットワーク エンジニアは、SPF に失敗したメッセージを検索して検疫に送信するには、コンテンツ フィルタを設定する必要があります。コンテンツ フィルタは設定され有効になっていますが、SPF に失敗したメッセージを除くすべてのメッセージが検疫に送信されます。この動作を修正するには、フィルタのどのセクションを変更する必要がありますか?
A. スキップフィルター
B. ログエントリ
C. SPF ステータス
D. 隔離
正解: **(正解を表示します)**
spf-status is the section of the filter that must be modified to correct this behavior. spf-status is a condition that determines whether a message matches the content filter rule based on the result of SPF verification, such as pass, fail, neutral, etc.
The content filter in the exhibit has a spf-status condition set to "Pass", which means that it will match messages that passed SPF verification and apply the action of "Quarantine". This is the opposite of what the network engineer intended to do.
To correct this behavior, the network engineer can modify the spf-status condition to "Fail", which means that it will match messages that failed SPF verification and apply the action of "Quarantine".
The other options are not valid sections of the filter that must be modified to correct this behavior, because they do not affect the spf-status condition.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 8-3 and page 8-4.

質問: **64**

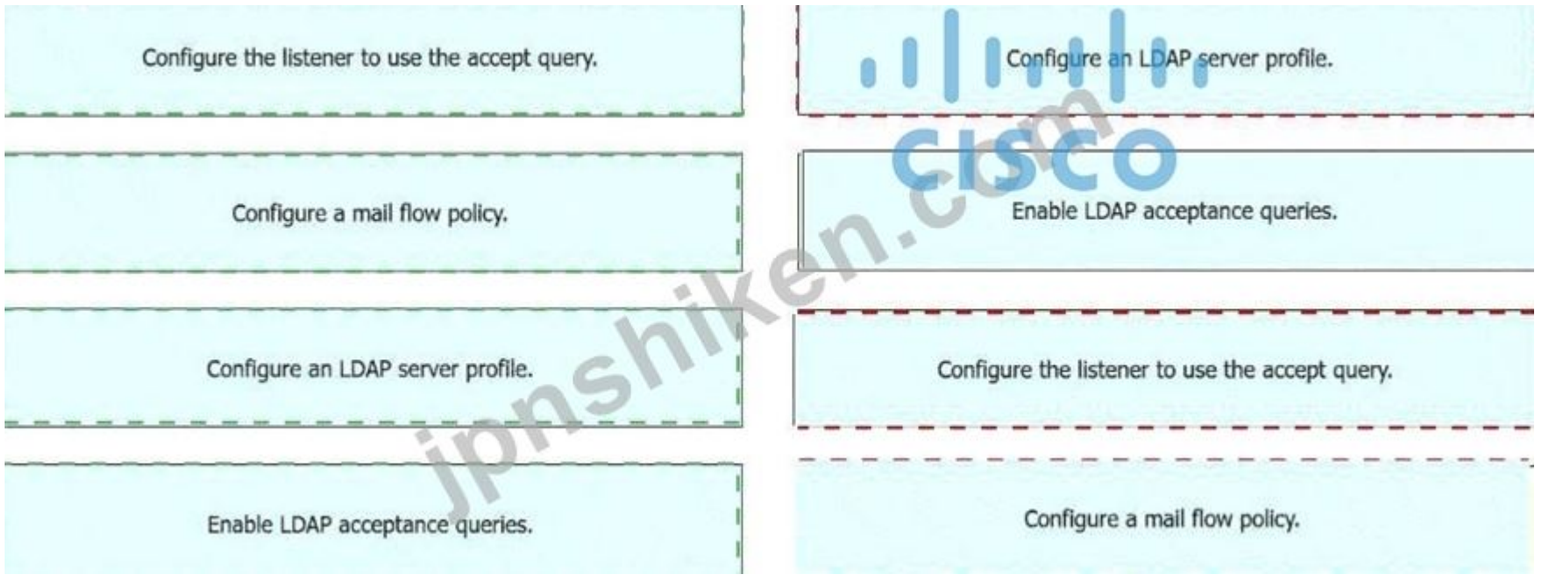
メッセージフィルター処理を構成するときに考慮する必要がある2つの要素はどれですか。 2つ選択してください。）
A. メッセージフィルターの順序
B. ラテラル加工
C. 結合されたパケットの構造
D. メールポリシー
E. メッセージのMIME構造
正解: (正解を表示します)
Message-filter order and MIME structure of the message are two factors that must be considered when message filter processing is configured on Cisco ESA. Message-filter 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.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 3-3 and page 3-5.
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_01000.html

質問: **65**
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. 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
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. スパム検疫エイリアス統合クエリ
正解: (正解を表示します)
Spam Quarantine End-User Authentication Query is a query that Cisco ESA performs against an LDAP server to validate the end-user credentials during login to the End-User Quarantine.
References: User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway , page 10-9.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure- esa-00.html

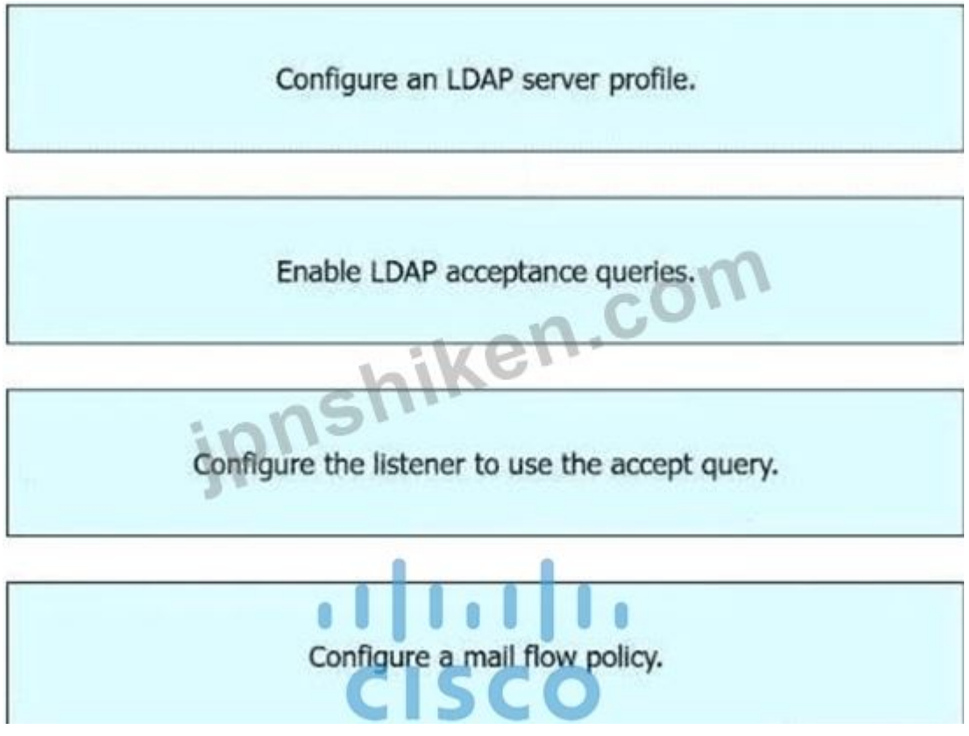
質問: **66**
Cisco Secure Email Gateway でディレクトリ収集防止を設定するには、左側のアクションを右側のシーケンスにドラッグアンドドロップします。



正解:

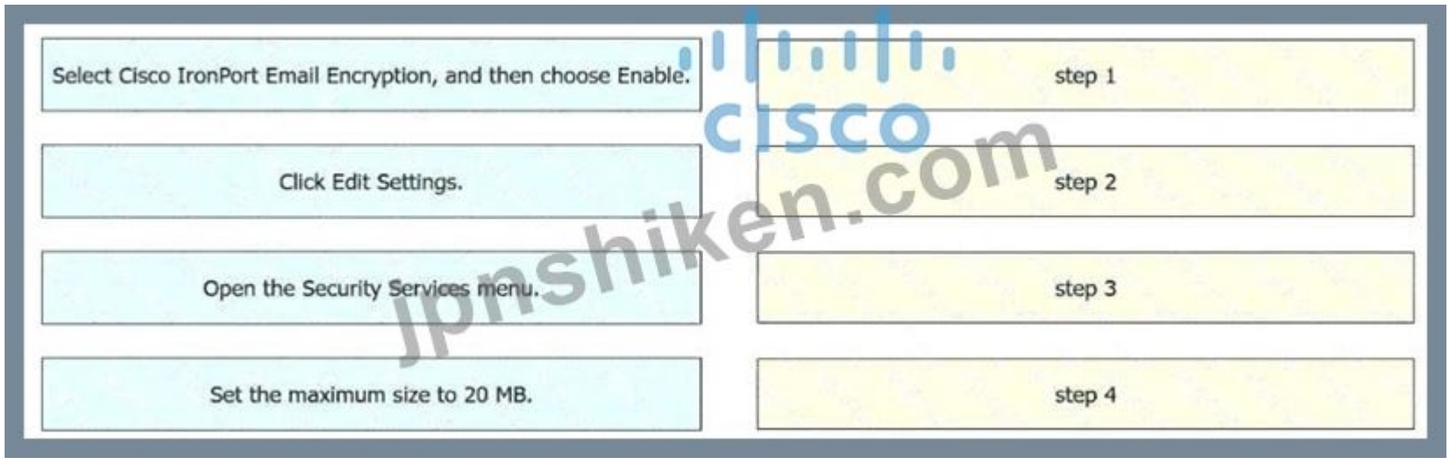


jpnshiken.com

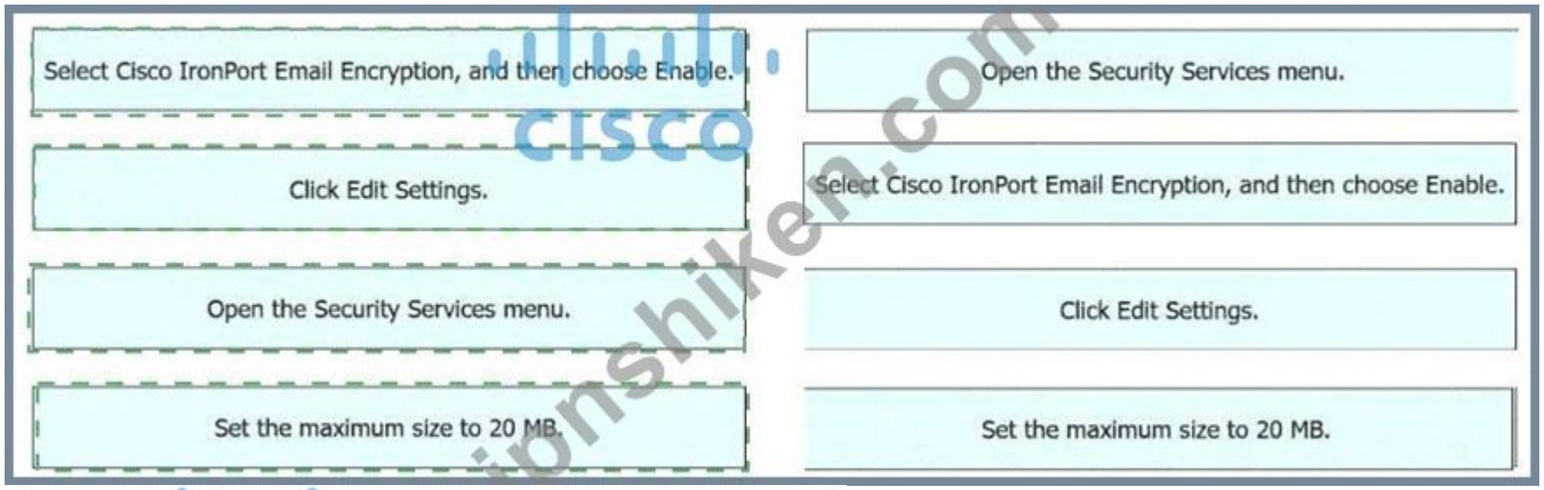


質問: **67**

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。



正解:



jpnshiken.com

Open the Security Services menu.

Select Cisco IronPort Email Encryption, and then choose Enable.

Click Edit Settings.

Set the maximum size to 20 MB.

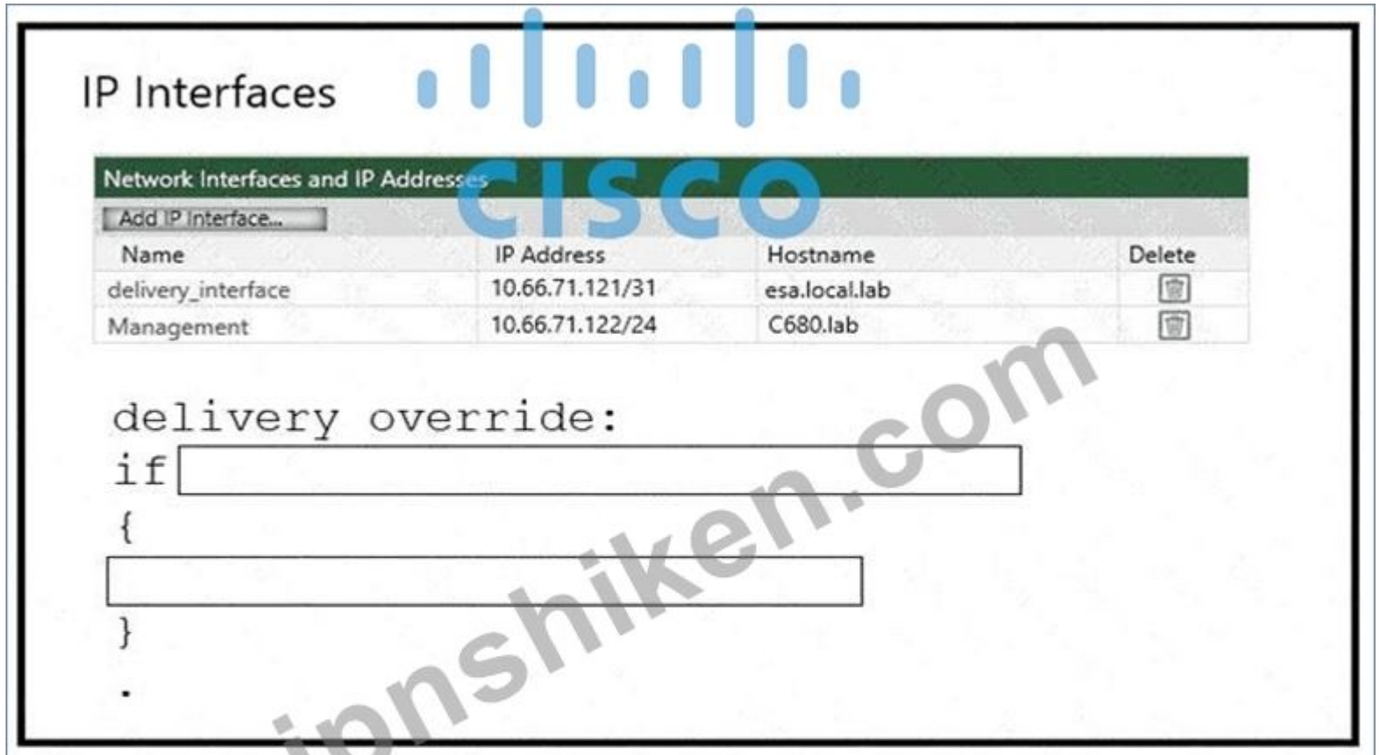
質問: **68**
管理者がウイルス以外の脅威にアウトブレイクフィルターを使用する前に、どの機能を設定する必要がありますか？
A. 隔離脅威レベル
B. スパム対策
C. データ損失防止
D. ウイルス対策
正解: **(**正解を表示します**)**
The feature that must be configured before an administrator can use the outbreak filter for nonviral threats is antispam. The outbreak filter relies on the antispam engine to detect and block nonviral threats, such as phishing, malware, or spam campaigns. You need to enable antispam scanning and configure the antispam settings before you can use the outbreak filter. References: Securing Email with Cisco Email Security Appliance (SESA) v3.1 , Module 8: Using Anti-Virus and Outbreak Filters, Lesson 2: Configuring Outbreak Filters 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_01110.html

質問: **69**
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: **D** (コメントを発表する)
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: **70**
管理者は、電子メールに cisco.com や test.com などの異なるドメインに複数の受信者がいる場合、特定の添付ファイルを含む受信電子メールがすべての受信者に配信されないことに気付きました。同じ電子メールが cisco.com の受信者にのみ送信された場合、適切に配信されます。この動作を回避するには、Cisco Secure Email Gateway をどのように設定する必要がありますか?
A. 電子メールがドロップされないように、cisco.com のメール ポリシーを変更します。
B. 電子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。
C. DLP 構成を変更して、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。
D. DLP 構成を変更して、test.com ドメインに送信されるメッセージの DLP スキャンを免除します。
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: **71**
管理者は、cisco_123@externally.com から送信された電子メールが代替仮想ゲートウェイを介してルーティングされることを確認する必要があります。スニペットを下部からグラフィック内の空白にドラッグ アンド ドロップして、メッセージ フィルター構文を完成させます。すべてのスニペットが使用されるわけではありません。



jpnshiken.com

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:

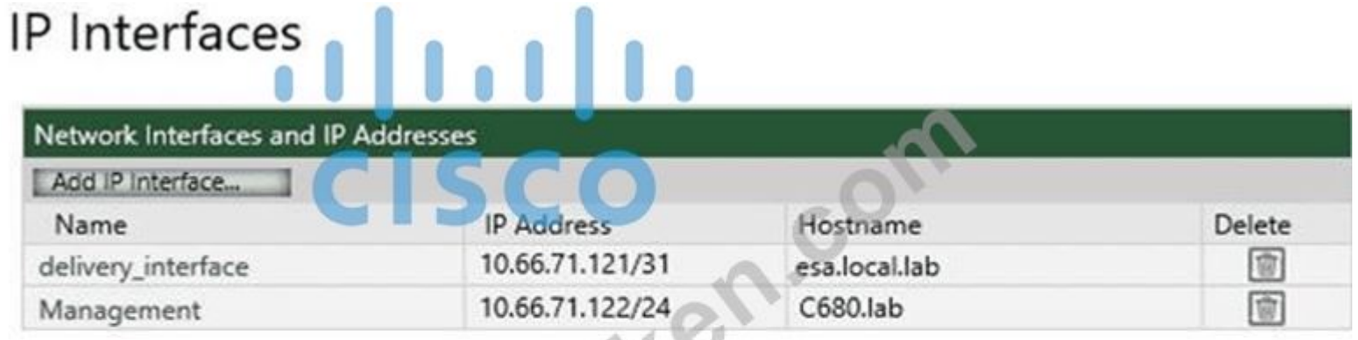



```
delivery override:
mail-from ==“cisco_123@externally.com”
{
livery-int(“delivery_interface”);
}
.
```

```
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”);
```

Explanation:

Table Description automatically generated




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

質問: 72

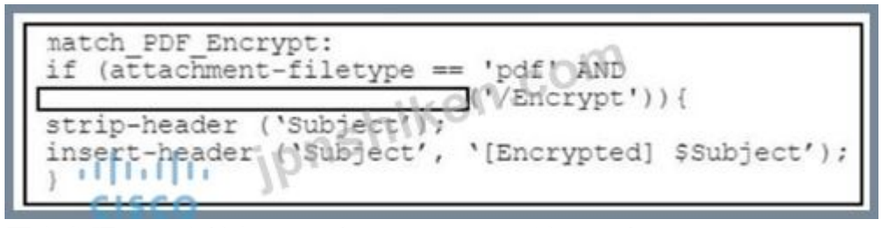
Cisco ESAで使用できる認証局リストはどれですか。 2つ選択してください。）
A. デフォルト
B. システム
C. ユーザー
D. カスタム
E. デモ
正解: (正解を表示します)
* System: This is the default list of trusted certificate authorities that is provided by Cisco and updated automatically. It contains the certificates of well-known and widely used certificate authorities, such as VeriSign, Thawte, and GoDaddy.
* Custom: This is the list of additional certificate authorities that you can add manually or import from a file. It allows you to trust certificates that are issued by your own or third-party certificate authorities that are not included in the system list.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/ b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_011000.html#task_1194859

質問: **73**
組織は、DNSレコードを活用して、DMARCを使用してブランドの評判を向上させたいと考えています。
このプロセスで使用される2つの電子メール認証メカニズムはどれですか？ 2つ選択してください。）
A. SPF
B. DSTP
C. DKIM
D. TLS
E. PKI
正解: (正解を表示します)
Reference:
https://www.cisco.com/c/en/us/products/security/what-is-dmarc.html
SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) are two email authentication mechanisms that are utilized during this process. SPF and DKIM allow the domain owner to publish DNS records that specify the authorized IP addresses or hosts for sending emails from that domain and sign the messages with a cryptographic key to prove their authenticity and integrity.
DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication standard that builds on SPF and DKIM and allows the domain owner to publish DNS records that specify how receivers should handle messages that fail SPF or DKIM verification, such as reject, quarantine, or none, and how to report back the results of DMARC validation.
The other options are not valid email authentication mechanisms that are utilized during this process, because they are not part of DMARC standard.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 11-2 and page 11-3.

質問: **74**
エンジニアは、Cisco Secure Email Gateway から Cisco SecureX へ脅威報告情報を共有する必要があります。
セキュアメールゲートウェイで有効にする必要がある設定はどれですか？
A. クラウドサービス設定
B. SNMP
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)

質問: **75**
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. 別名統合クエリ
C. LDAP認証クエリ
D. 外部認証クエリ
正解: **(**正解を表示します**)**

質問: **76**



図を参照してください。セキュリティエンジニアは、Cisco Secure Email Gateway 上にメッセージフィルタを作成し、受信メールすべてをスキャンして暗号化された PDF ファイルを検出する必要があります。どのコードスニペットがメッセージフィルタを完成させますか？
A. 添付ファイル
B. 添付ファイルバイナリが含まれています
C. 添付ファイルバイナリファイル
D. attachment-binary-include
正解: **B (**コメントを発表する**)**

有効的な**300-720J**問題集はJPNTest.com提供され、**300-720J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-720J**試験問題集を提供します。JPNTest.com 300-720J試験問題集はもう更新されました。ここで**300-720J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-720J-mondaishu　**244**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
管理者は、過去1週間に、Cisco ESAが、一貫して隔離されている特定の送信者およびドメインから多くの電子メールを受信していることを確認しました。管理者は、これらの送信者とドメインがこれ以上電子メールを送信できないようにする必要があります。
これを実現するには、Cisco ESAのどの機能を使用する必要がありますか？
A. 受信メールポリシー
B. セーフリスト
C. ブロックリスト
D. S / MIME送信プロファイル
正解: **(**正解を表示します**)**
The appliance enforces your organization's policies for messages sent to and from your users through the use of mail policies. These are sets of rules that specify the types of suspect, sensitive, or malicious content that your organization may not want entering or leaving your network. This content may include:
-spam

-legitimate marketing messages
-graymail
-viruses
-phishing and other targeted mail attacks
-confidential corporate data
-personally identifiable information
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?bookSearch=true

質問: **78**
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**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0
/b_ESA_Admi n_Guide_12_0_chapter_011010.html
DHAP (Directory Harvest Attack Prevention) is a feature that must be used to address this issue. DHAP is a mechanism that allows Cisco ESA to prevent directory harvest attacks, which are attempts by spammers or hackers to obtain valid email addresses from an LDAP server by sending messages with random or guessed recipients and checking for bounce messages.
To enable DHAP on Cisco ESA, the network administrator can follow these steps:
Select Network > Listeners and click Edit Settings for the listener that receives incoming messages.
Under SMTP Authentication Settings, select Enable Directory Harvest Attack Prevention.
Enter a value for Maximum Invalid Recipients per Hour, which is the number of invalid recipients that triggers DHAP.
Enter a value for Block Sender for (hours), which is the duration that Cisco ESA blocks messages from senders who exceed the maximum invalid recipients per hour.
Click Submit.

質問: **79**
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。この要件を満たすには、どのような対策を講じ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. 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。
C. ドメインをセーフリストに追加します。
D. Wockリストからドメインを削除します。
正解: **C (**コメントを発表する**)**

質問: **80**
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: **(**正解を表示します**)**
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.
The other options are not valid actions to resolve the issue, because they do not affect the port used by AMP file reputation.
References: [User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway], page 7-5 and page 7-6.

質問: **81**
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**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/e sa12-0/user_guide/b_ESA_Admin_Guide_12_0
/b_ESA_Admin_Guide_12_0_chapter_011001.html
one of the steps to accept mail for additional i nternal domains on the Cisco ESA is to choose Network > SMTP Routes and enter the new domain and the corresponding destination host IP address 1 . This can also be done using the smtproutes command in the CLI 1 . The other commands (deliveryconfig, dsestconf, and altrchost) are not related to this task.

質問: **82**
グレイメールサービスの利点は何ですか？
A. 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
B. ソーシャルネットワークのメールを安全に購読する方法を提供します
C. クラウドおよびオンサイトの解約サービスを提供
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**)**

質問: **83**
HTTPS 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. References : [Cisco Secure Email Gateway Administrator Guide - Configuring Certificates]

質問: **84**
エンジニアは、疑わしいスパムメッセージが役員グループに配信されないように、Cisco Secure Email Gateway にポリシーを実装する必要があります。Yahoo! などの公開電子メール アドレスから届くメッセージ。
.com または gmail.com ドメインは、IT 部門にリダイレクトする必要があります。この要件を満たすために実行する必要のある設定アクションはどれですか？(2つ選択してください。)
A. 送信者ドメインを受信者として executives.com に一致させるメール ポリシーを実装します。
B. 電子メール アドレスまたは LDAP グループを介してエグゼクティブ 受信者に一致するようにポリシーを設定します。
C. メールポリシーを適用して、送信者ドメインを役員ではなく送信者として一致させます。
D. 送信者ドメインを @yahoo.com および @gmail.com に一致させるメールポリシーを追加します。
E. 送信者ドメインを「yahoo.com」および「gmail.com」として一致させるメールポリシーを設定します。
正解: **(**正解を表示します**)**

質問: **85**
SPF/SIDF 検証を使用するように Cisco ESA を設定する手順を左側から右側の正しい順序にドラッグ アンド ドロップします。



正解:

Associate the filter with a nominated incoming mail policy.	Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.
Configure a filter to take necessary action on SPF/SIDF verification results.	Configure a sendergroup to use the custom mail-flow policy.
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	Associate the filter with a nominated incoming mail policy.
Test the results of message verification.	Configure a filter to take necessary action on SPF/SIDF verification results.
Configure a sendergroup to use the custom mail-flow policy.	Test the results of message verification.

Associate the filter with a nominated incoming mail policy.	Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.
Configure a filter to take necessary action on SPF/SIDF verification results.	Configure a sendergroup to use the custom mail-flow policy.
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	Associate the filter with a nominated incoming mail policy.
Test the results of message verification.	Configure a filter to take necessary action on SPF/SIDF verification results.
Configure a sendergroup to use the custom mail-flow policy.	Test the results of message verification.

有効的な**300-720J**問題集はJPNTest.com提供され、**300-720J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-720J**試験問題集を提供します。JPNTest.com 300-720J試験問題集はもう更新されました。ここで**300-720J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-720J-mondaishu **244**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」