

Cisco.300-710J.v2021-11-26.q62

試験コード : 300-710J
試験名称 : Securing Networks with Cisco Firepower (300-710日本語版)
認証ベンダー : Cisco
無料問題の数 : 62
バージョン : v2021-11-26
ページの閲覧量 : 595
問題集の閲覧量 : 5591

<https://www.jpnsiken.com/shiken/Cisco.300-710J.v2021-11-26.q62.html>

質問: 1

管理者がSNORT検査ポリシーを設定していて、CiscoFMCに失敗した展開メッセージが表示されています。管理者は、トラブルシューティングに役立つCisco TAC用にどのような情報を生成する必要がありますか？

- A. A Troubleshoot" file for the device in question.
- B. A "troubleshoot" file for the Cisco FMC
- C. A "show tech" file for the device in question
- D. A "show tech" for the Cisco FMC.

正解: ([正解を表示します](#))

質問: 2

エンジニアは、CiscoFMCでネットワーク検出ポリシーを設定します。設定時に、データベースをファイリングし、CiscoFMCに過負荷をかける過度で誤解を招くイベントに気づきました。監視対象のNATデバイスは、オペレーティングシステムの複数の更新を短時間で実行しています。この問題を軽減するには、どのような構成変更を行う必要がありますか？

- A. デフォルトのネットワークのままにします。
- B. NATデバイスのエントリ数を増やします。
- C. メソッドをTCP / SYNに変更します。
- D. ロードバランサーとNATデバイスを除外します。

正解: ([正解を表示します](#))

質問: 3

組織は、Cisco Firepowerデバイスを使用して、ブランチオフィスから本社ビルへのトラフィックを保護したいと考えています。CiscoFirepowerデバイスがVPNトラフィックの検査にリソースを浪費していないことを確認したいと考えています。これらの要件を満たすために何をする必要がありますか？

- A. VPNトラフィックが検査なしで通過できるように、侵入ポリシーを調整します
- B. プレフィルタポリシーを使用してVPNトラフィックを無視するようにCiscoFirepowerデバイスを設定します

C. flexconfigポリシーを有効にして、VPNトラフィックを再分類し、対象のトラフィックとして表示されないようにします。

D. VPNトラフィックのアクセス制御ポリシーをバイパスするようにCiscoFirepowerデバイスを設定します。

正解: [\(正解を表示します\)](#)

質問: 4

アナリストは、その週のCiscoFMCレポートを確認しています。彼らは、いくつかのピアツーピアアプリケーションがネットワーク上で使用されていることに気づき、環境に最大のリスクをもたらすものを特定する必要があります。アナリストにこの情報を提供するレポートはどれですか？

A. ネットワークリスクレポート

B. ユーザーリスクレポート

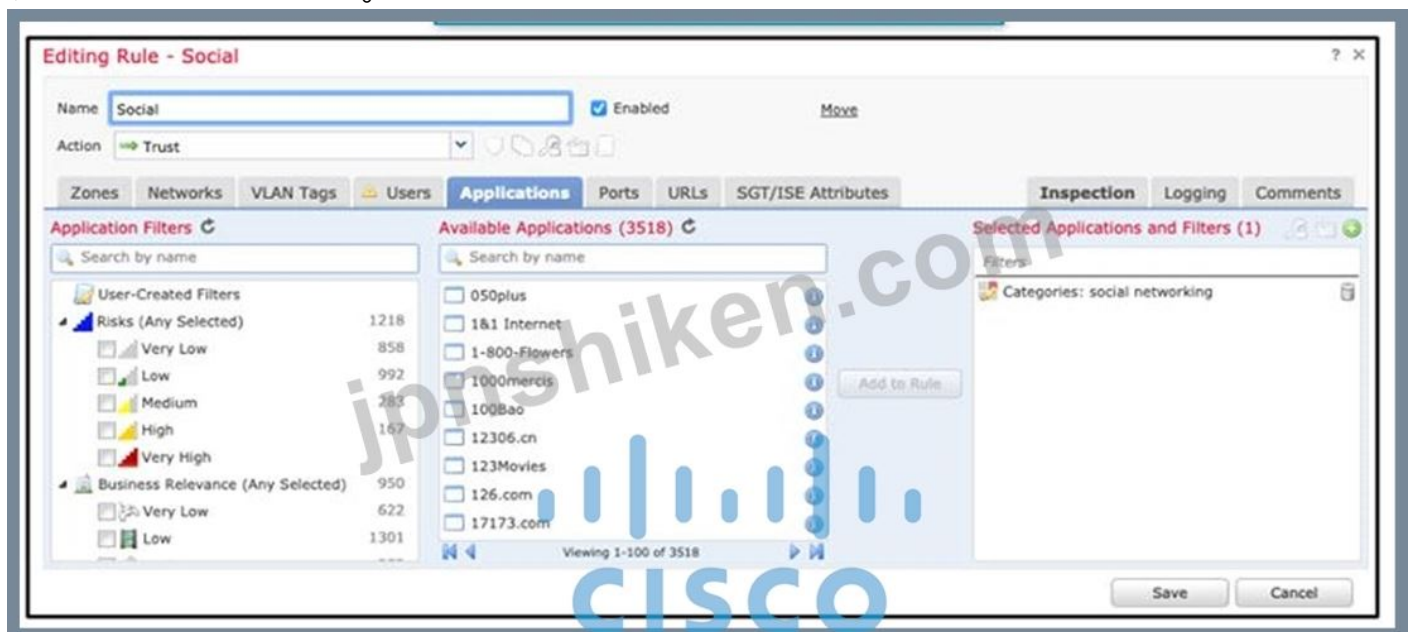
C. 高度なマルウェアリスクレポート

D. 攻撃リスクレポート

正解: [\(正解を表示します\)](#)

質問: 5

展示を参照してください。



組織には、検査のためにすべてのソーシャルメディアトラフィックを送信することを目的としたアクセス制御ルールがあります。ルールをしばらく使用した後、管理者はトラフィックが検査されていないことに気が付きますが、自動的に許可されますこの問題に対処するにはどうすればよいですか？

A. ルールアクションを信頼から変更して許可する

B. ルール内で選択したアプリケーションを変更します

C. 侵入ポリシーをセキュリティを介した接続に変更します。

D. ソーシャルネットワークのURLをブロックリストに追加します

正解: [\(正解を表示します\)](#)

質問: 6

組織内のネットワークデバイスを管理および監視するためのネットワーク監視ツールを導入した後、Cisco FMCのMIBを手動でアップロードする必要があることに気付きました。どのフォルダにMIBファイルをアップロードしますか？

- A. /etc/sf/DCMIB.ALERT
- B. system/etc/DCEALERT.MIB
- C. /sf/etc/DCEALERT.MIB
- D. /etc/sf/DCEALERT.MIB

正解: ([正解を表示します](#))

質問: 7

Cisco FTDデバイスは、VTEPブリッジグループメンバーの入カインターフェイスを備えた透過ファイアウォールモードで実行されています。パケットトレースの宛先MACアドレスの指定を担当するエンジニアは、何を考慮する必要がありますか。

- A. VLANIDと宛先MACアドレスはオプションです
- B. パケットログの出力形式オプションは使用できません
- C. VLAN ID値が入力されている場合、宛先MACアドレスはオプションです
- D. UDPパケットタイプのみがサポートされています

正解: **C** ([コメントを發表する](#))

質問: 8

組織は、マルチコンテキストモードで実行されているCiscoASAデバイスをCiscoFTDデバイスに移行しています。CiscoASAの各コンテキストがCiscoFTDデバイスで論理的に分離されていることを確認するには、どのアクションを実行する必要がありますか。

- A. ネイティブインスタンスを追加して、各CiscoFTDコンテキストにトラフィックを分散します。
- B. CiscoFTDデバイスをCiscoASAポートチャネルに追加します。
- C. 複数のネットワークにまたがるポートチャネルを使用するようにCiscoFTDを設定します。
- D. Cisco ASAのコンテキストごとに、CiscoFTDでコンテナインスタンスを設定します。

正解: **B** ([コメントを發表する](#))

質問: 9

デバイスの削除とCisco FMCへの再追加について正しいのは次のうちどれですか。(2つ選択してください。)

- A. 登録時にNATおよびVPNポリシーを再適用するオプションが利用できるため、ユーザーは登録の完了後にポリシーを再適用する必要はありません。
- B. Cisco FMC Webインターフェイスは、アクセス制御ポリシーを再適用するようにユーザーに促します。
- C. Cisco FMCにデバイスを再度追加する前に、デバイスにマネージャを追加する必要があります。

D. 登録時にNATおよびVPNポリシーを再適用するオプションは利用できないため、ユーザーは登録の完了後にポリシーを再適用する必要があります。

E. Cisco FMC Webインターフェイスでは、デバイスを削除して再度追加するオプションはありません。

正解: **B,D** ([コメントを發表する](#))

質問: 10

エンジニアは、子ドメインでCiscoFMCダッシュボードを設定する必要があります。ダッシュボードが親ドメインに表示されるようにするには、どのアクションを実行する必要がありますか？

- A. 別のタブを追加します。
- B. 別のウィジェットを追加します。
- C. ダッシュボードのコピーを作成します。
- D. ポリシーの継承設定を調整します。

正解: ([正解を表示します](#))

質問: 11

ファイアウォールが同じサブネットのレイヤー2とレイヤー3でトラフィックを転送できるようにするファイアウォール設計はどれですか？

- A. Cisco Firepower ThreatDefenseモード
- B. ルーテッドモード
- C. 統合されたルーティングとブリッジング
- D. 透過モード

正解: **A** ([コメントを發表する](#))

質問: 12

組織には、ブリッジグループを使用してトラフィックを内部インターフェイスから外部インターフェイスに渡すCiscoFTDがあります。隣接するCiscoデバイスに関する情報を収集したり、環境でマルチキャストを使用したりすることはできません。この問題を解決するには何をする必要がありますか？

- A. ファイアウォールモードを透過に変更します。
- B. CDPトラフィックを許可するファイアウォールルールを作成します。
- C. ファイアウォールインターフェイスを使用してブリッジグループを作成します。
- D. ファイアウォールモードをルーテッドに変更します。

正解: ([正解を表示します](#))

質問: 13

エンジニアは、CiscoFMGでコマンドrestoreremote-manager-backup location 1.1.1.1 admin / volume / home / admin BACKUP_Cisc394602314.zipを使用して、リモートバックアップからCiscoFTD設定を復元しています。リポジトリに接続した後、FTDデバイスがバックアップファイルを受け入れるのを妨げるエラーが発生しました。何が問題ですか？

- A. バックアップファイルが.cfg形式ではありません。
- B. バックアップファイルの拡張子がtarからzipに変更されました
- C. バックアップファイルがCiscoFTDデバイスに対して大きすぎます
- D. バックアップファイルが適用される前に有効化されていませんでした

正解: ([正解を表示します](#))

質問: 14

ある企業は、CiscoFMCによって管理されているCiscoFTDを使用して侵入防止を展開している最中です。エンジニアは、潜在的な侵入を検出するが、疑わしいトラフィックをブロックしないようにポリシーを構成する必要があります。どのアクションがこのタスクを実行しますか？

- A. [AccessPolicies]セクションの[CiscoFMC Intrusion]タブでポリシールールを作成または編集するときに、[Drop when inline]オプションをオフにしてIPSモードを設定します。
- B. [AccessPolicies]セクションの[CiscoFMC Intrusion]タブで、[Drop when inline]オプションをオンにして、ポリシールールを作成または編集するときにIPSモードを設定します。
- C. [AccessPolicies]セクションの[CiscoFMC Intrusion]タブでポリシールールを作成または編集するときに、[Drop when inline]オプションをオフにしてIDSモードを設定します。
- D. [AccessPolicies]セクションの[CiscoFMC Intrusion]タブで、[Drop when inline]オプションをオンにして、ポリシールールを作成または編集するときにIDSモードを設定します。

正解: ([正解を表示します](#))

質問: 15

組織は、動作分析のために、CiscoFTDデバイスからCiscoStealthwatchにNetFlowトラフィックを取り込むことができる必要があります。この要件を満たすには、Cisco FTDで何を設定する必要がありますか？

- A. NetFlowのflexconfigオブジェクト
- B. NetFlowの変数セットオブジェクト
- C. NetFlowをエクスポートするためのインターフェースオブジェクト
- D. NetFlowのセキュリティインテリジェンスオブジェクト

正解: ([正解を表示します](#))

質問: 16

エンジニアは、複数のDMZをサポートする内部境界ファイアウォールを展開する必要があります。各DMZには、一意のプライベートIPサブネット範囲があります。この要件はどのように満たされますか？

- A. NATが構成された透過モードでファイアウォールを展開します。
- B. アクセス制御ポリシーを使用してファイアウォールを透過モードで展開します。
- C. NATが構成されたルーテッドモードでファイアウォールを展開します。
- D. アクセス制御ポリシーを使用してファイアウォールをルーテッドモードで展開します。

正解: ([正解を表示します](#))

有効的な**300-710J**問題集はJPNTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-710J**試験問題集を提供します。JPNTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**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/300-710J-mondaishu> **578**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

Cisco Firepowerでファイアウォールデバッグメッセージを生成するために使用されるCLIコマンドはどれですか。

- A. system support dump-table
- B. system support ssl-debug
- C. system support firewall-engine-debug
- D. system support platform

正解: ([正解を表示します](#))

質問: 18

Syslogを使用するのではなく、CiscoFirepowerデバイスがセキュリティサービス交換ポータルを介してCiscoThreat応答にイベントを直接送信することの利点は何ですか。

- A. Firepowerデバイスはインターネットに接続する必要はありません。
- B. すべてのタイプのFirepowerデバイスがサポートされています。
- C. サポートされているバージョンのFirepowerを実行しているすべてのデバイスをサポートします
- D. オンプレミスプロキシサーバーをセットアップして維持する必要はありません

正解: ([正解を表示します](#))

Reference:

Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

質問: 19

マルチドメイン環境のCisco Firepower Management Centerダッシュボードに適用される制限はどれですか。

- A. 子ドメインは、祖先ドメインからの限られたウィジェットセットにのみアクセスできます。
- B. 子ドメインは、祖先ドメインに由来するダッシュボードを表示できませんが編集はできません。
- C. 子ドメインは、祖先ドメインに由来するダッシュボードを表示できません。
- D. 最上位の祖先ドメインの管理者のみがダッシュボードを表示できます。

正解: ([正解を表示します](#))

質問: 20

セキュリティエンジニアは、複数のブランチロケーションのアクセス制御ポリシーを構成しています。これらのロケーションは、共通のルールセットを共有し、各ロケーションでローカルに重要な内部ネットワークサブネットを含むINSIDE_NETと呼ばれるネットワークオブジェクトを利用します。各ロケーションでポリシーの一貫性を維持しながら、該当するルール内のローカルで重要なネットワークサブネットのみ？

- A. INSIDE_NETネットワークオブジェクトとオブジェクトオーバーライドを使用してACPを作成する
- B. ポリシーの継承を利用する
- C. CiscoTalosから更新される動的ACPを利用する
- D. デバイスごとに一意のACPを作成する

正解: ([正解を表示します](#))

質問: 21

ネットワークセキュリティエンジニアは、問題のトラブルシューティング中に、Cisco FMCWebブラウザからパケットキャプチャをエクスポートする必要があります。アドレスに移動するときエラー！ハイパーリンク参照が無効です。IP> /capture/CAP/pcap/test.pcap。エラー403 :PCAPファイルの代わりにForbiddenが指定されています。この問題を解決するには、エンジニアはどのアクションを実行する必要がありますか？

- A. HTTPSサーバーを無効にし、代わりにHTTPを使用します。
- B. ブラウザのプロキシサーバー設定としてCisco FTDIPアドレスを使用します。
- C. デバイスプラットフォームポリシーのHTTPSサーバーを有効にします。
- D. ブラウザのプロキシ設定を無効にします。

正解: ([正解を表示します](#))

質問: 22

ネットワークエンジニアは、侵入検知機能を利用するために、ネットワーク上に新しいCiscoFirepowerデバイスを実装します。デバイスを通るトラフィックを分析し、悪意のあるトラフィックを警告し、ネットワークのバンプとして表示する必要があります。これをどのように実装する必要がありますか？

- A. CiscoFirepowerでルーティングを有効にします
- B. 物理CiscoFirepowerインターフェイスにIPアドレスを追加します。
- C. ブリッジグループを透過モードで構成します。
- D. 接続されたデバイスのデフォルトゲートウェイとしてBVIIPアドレスを指定します。

正解: **B** ([コメントを發表する](#))

質問: 23

複数のドメインが使用されているマルチテナント展開。グローバルドメインの外部でどの更新を適用する必要がありますか？

- A. Ciscoジオロケーションデータベース
- B. マイナーアップグレード

- C. メジャーアップグレードのローカルインポート
- D. 侵入ルールのローカルインポート

正解: [\(正解を表示します\)](#)

質問: 24

Which two packet captures does the FTD LINA engine support?

- A. application ID
- B. Layer 7 network ID
- C. protocol
- D. source IP
- E. dynamic firewall importing

正解: C,D ([コメントを发表する](#))

質問: 25

Cisco FMCで設定され、Cisco FTDに伝達されるOSPFルーティング機能はどれですか。(2つ選択してください。)

- A. エリア境界ルータータイプ1 LSAフィルタリング
- B. OSPFパケットに対するMD5認証
- C. IPv6機能を備えたOSPFv2
- D. OSPFパケットに対するSHA認証
- E. 仮想リンク

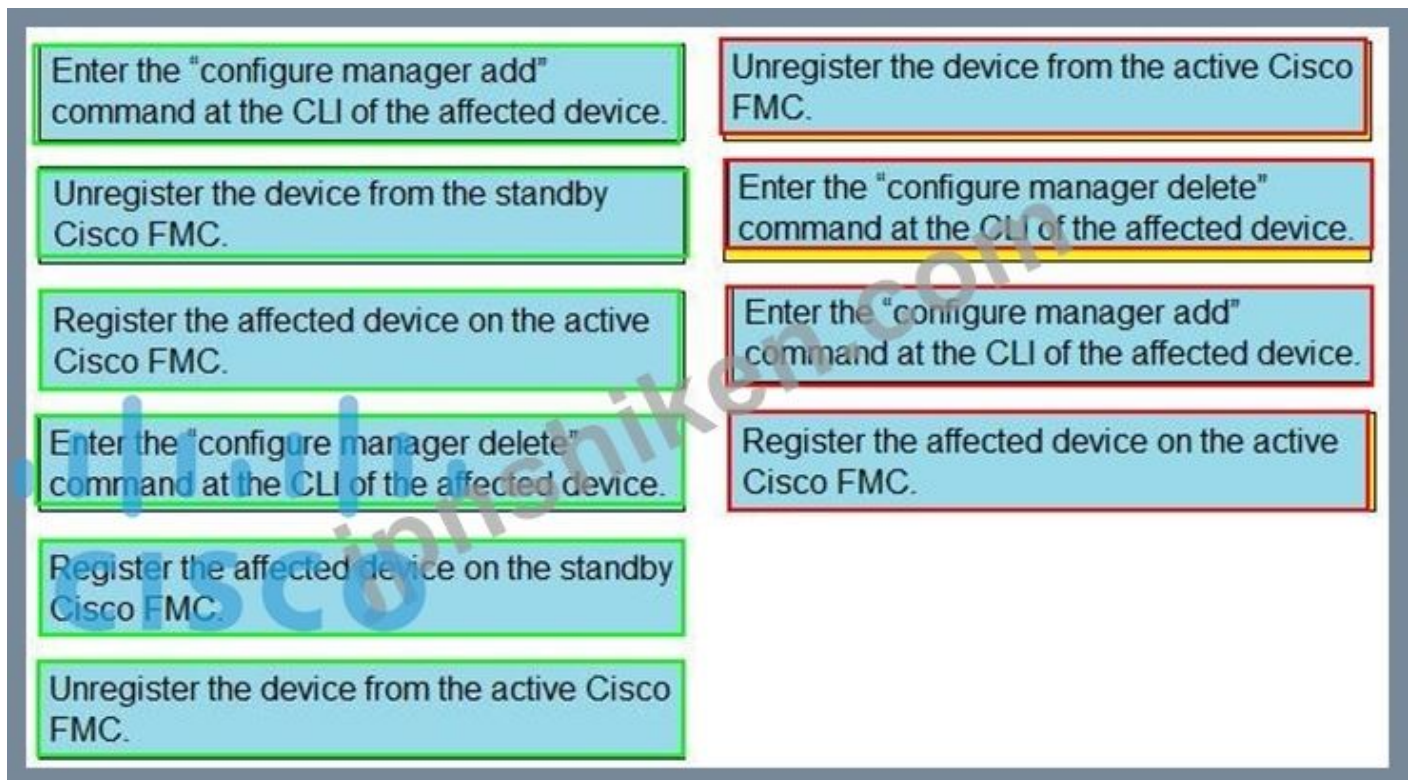
正解: [\(正解を表示します\)](#)

質問: 26

手順をドラッグアンドドロップして、スタンバイCiscoFMCでの自動デバイス登録の失敗を左側から右側の正しい順序に復元します。すべてのオプションが使用されるわけではありません。

Enter the "configure manager add" command at the CLI of the affected device.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

正解:



質問: 27

エンドポイントをアクティブに監視するためにのみ使用されるCisco Advanced Malware Protection for Endpointsポリシーはどれですか？

- A. Windowsドメインコントローラ
- B. 保護
- C. 監査
- トリアージ

正解: ([正解を表示します](#))

質問: 28

Cisco FMCデータベースパージの動作は何ですか。

- A. 指定されたデータはCisco FMCから削除され、2週間保持されます。
- B. User Activityチェックボックスがオンの場合、ユーザログインと履歴データはデータベースから削除されます。
- C. 適切なプロセスが再起動されます。
- D. データはデバイスから復元できます。

正解: ([正解を表示します](#))

質問: 29

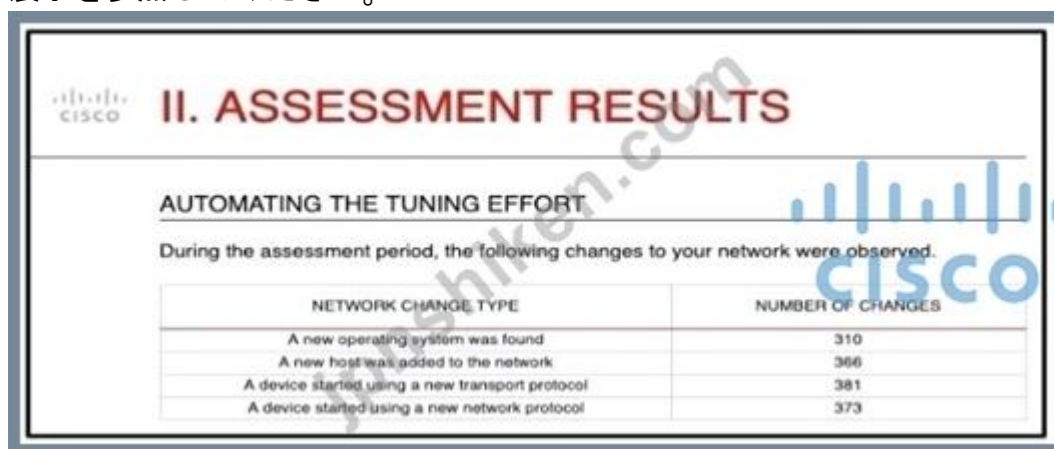
管理者は、ユーザーがクラウドでホストされているWebサーバーにアクセスできないというレポートを受け取ります。アクセス制御ポリシーは最近、いくつかの新しいポリシーの追加とURLフィルタリングで更新されました。組織のセキュリティ体制を犠牲にすることなく、問題のトラブルシューティングとアクセスの復元を行うには、何をする必要がありますか？

- A. Cisco FMC接続イベントでブロックされたトラフィックを特定してブロックを検証し、ポリシーを変更してWebサーバーへのトラフィックを許可します。
- B. パケットキャプチャツールを使用してブロックを確認し、トラフィックのアクションモニターを使用してルールを作成します。
- C. トラフィックのPCAPをダウンロードしてブロックを検証し、flexconfigオブジェクトを使用して、宛先サーバーへの必要なトラフィックのみを許可するルールを作成します。
- D. 新しいアクセス制御ポリシールールを作成して、WebサーバーのFQDNへのポート80および443を許可します。

正解: ([正解を表示します](#))

質問: 30

展示を参照してください。



The screenshot displays a slide titled "II. ASSESSMENT RESULTS" with the subtitle "AUTOMATING THE TUNING EFFORT". It states: "During the assessment period, the following changes to your network were observed." Below this is a table with two columns: "NETWORK CHANGE TYPE" and "NUMBER OF CHANGES".

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

また、エンジニアは攻撃リスクレポートを分析しており、ネットワーク上に新しいオペレーティングシステムのインスタンスが300を超えていることを発見しました。これらの新しいオペレーティングシステムを保護するためにFirepower構成はどのように更新されますか？

- A. CiscoFirepowerはポリシーを自動的に更新します。
- B. 管理者がCiscoFirepowerに修復推奨レポートを要求します
- C. Cisco Firepowerは、ポリシーを更新するための推奨事項を提供します。
- D. 管理者は手動でポリシーを更新します。

正解: ([正解を表示します](#))

Ref: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailoring_Intrusion_Protection_to_Your_Network_Assets.html

質問: 31

クラスター化ユニット環境でサイト間VPNを設定することの欠点は何ですか？

- A. 新しいマスターユニットが選出された場合、VPN接続を再確立する必要があります。
- B. すべてのクラスターユニットで同時にVPN接続を維持するには、スマートライセンスが必要です。
- C. 新しいマスターユニットが選出されると、確立されたVPN接続のみが維持されます。
- D. VPN接続は、障害が発生したマスターユニットが回復した場合にのみ再確立できます。

正解: ([正解を表示します](#))

有効的な**300-710J**問題集はJPNTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-710J**試験問題集を提供します。JPNTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**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/300-710J-mondaishu> **578**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

Cisco FTDのブリッジグループインターフェイスに関する2つのステートメントが正しいですか。(2つ選択してください。)

- A. 直接接続された各ネットワークは同じサブネット上にある必要があります。
- B. BVI IPアドレスは、接続されたネットワークとは別のサブネットにある必要があります。
- C. 双方向フォワーディング検出エコーパケットは、ブリッジグループメンバーを使用する場合、FTDを介して許可されます。
- D. ブリッジグループは、透過ファイアウォールモードとルーテッドファイアウォールモードの両方でサポートされています。
- E. ブリッジグループは、透過ファイアウォールモードでのみサポートされます。

正解: **A,D** ([コメントを發表する](#))

質問: 33

ネットワーク管理者は先月のファイルレポートを確認し、exeを除くすべてのファイルタイプに気づきました。未知の性質を示します。この問題の原因は何ですか？

- A. マルウェアライセンスはCiscoFTDに適用されていません。
- B. ファイルポリシーがアクセスポリシーに適用されていません。
- C. Speroファイル分析のみが有効になります。
- D. Cisco FMCは、ファイルを分析するためにインターネットにアクセスできません。

正解: ([正解を表示します](#))

質問: 34

Threat Intelligence Directorがサポートするフィルタリングの最大SHAレベルはいくつですか？

- A. SHA-512
- B. SHA-4096
- C. SHA-1024
- D. SHA-256

正解: **D** ([コメントを發表する](#))

質問: 35

Cisco FMCのポートオブジェクトの機能は何ですか。

- A. ルールで送信元と宛先の両方のポート条件を設定するときにトランスポートプロトコルを混在させる
 - B. TCP、UDP、およびICMP以外のプロトコルを表す
 - C. アクセスコントロールルールのソースポート条件にTCPまたはUDP以外のプロトコルを追加する。
 - D. すべてのプロトコルを同じ方法で表す
- 正解: **B** ([コメントを發表する](#))

質問: 36

エンジニアは、Cisco Firepower デバイスのハイアベイラビリティを設定する必要があります。現在のネットワークトポロジでは、2つのデバイスが同時にトラフィックを通過させることはできません。この環境でデバイスをどのように実装する必要がありますか？

- A. in a cluster span EtherChannel
 - B. in active/passive mode
 - C. in active/active mode
 - D. in cluster interface mode
- 正解: ([正解を表示します](#))

質問: 37

Cisco FMCpxGridと統合するためにCisco ISEで必要なライセンスタイプはどれですか。

- A. 頂点
 - B. プラス
 - C. ベース
 - D. モビリティ
- 正解: **B** ([コメントを發表する](#))

質問: 38

エンジニアが Cisco FMC 内に新しいダッシュボードを作成して、他の多くのダッシュボードからのウィジェットを1つのビューに表示しようとしています。目標は、脅威とセキュリティ関連のウィジェットと Cisco Firepower デバイスのヘルス情報を混在させることです。この情報を提供するには、どの2つのウィジェットを構成する必要がありますか？ (2つ選んでください)。

- A. ネットワークコンプライアンス
 - B. 相関情報
 - C. 現在のセッション
 - D. アプライアンスのステータス
 - E. 侵入イベント
- 正解: **B,E** ([コメントを發表する](#))

質問: 39

エンジニアは、新しいCiscoFTDデバイスの背後にあるホストからDNSサーバへの接続のトラブルシューティングを行っています。ホストは、DMZ内のサーバーにDNSクエリを送信できません。実際のDNSパケットを使用してこの問題をトラブルシューティングするには、エンジニアはどのアクションを実行する必要がありますか？

- A. パケットトレーサツールを使用して、パケットがドロップされているホップを判別します。
- B. 接続イベントダッシュボードを使用して、ブロックの理由を確認し、必要に応じて検査ポリシーを調整します。
- C. Threat DefenseCLIツールのshowblocksコマンドを使用して、ブロックされたトラフィックを許可するポリシーを作成します。
- D. パケットキャプチャツールを使用して、トラフィックがブロックされている場所を確認し、必要に応じてアクセス制御または侵入ポリシーを調整します。

正解: ([正解を表示します](#))

質問: 40

管理者は、ポリシー内で使用するために、新しいURLベースのカテゴリフィードをCiscoFMCに追加しています。インテリジェンスソースはSTIXを使用しません。ただし、代わりに.txtファイル形式を使用します。定期的な更新が確実に提供されるようにするアクションはどれですか？

- A. txtファイルをアップロードし、埋め込まれたURLを使用して自動更新を構成します。
- B. txtファイルをSTIXに変換し、CiscoFMCにアップロードします。
- C. TAXIIフィードソースを追加し、フィードのURLを入力します。
- D. URLソースを追加し、CiscoFMC内でフラットファイルタイプを選択します。

正解: C ([コメントを发表する](#))

質問: 41

アクセスコントロールポリシールールで使用できる2つのアクションはどれですか。(2つ選択してください。)

- A. すべてをブロック
- B. 分析
- C. リセット付きブロック
- D. 発見
- E. モニター

正解: ([正解を表示します](#))

質問: 42

展示を参照してください。



エンジニアは、アクセス制御ポリシーを変更して、パスするすべてのDNSトラフィックを検査するルールを追加し、ポリシーを変更して展開しています。DNSトラフィックがSnortエンジンによって検査されていないことがわかります。とは.....

- A. ルールが送信元ポートの間違った設定で構成されています。
- B. ルールは、トラフィックを発信するセキュリティゾーンを指定する必要があります。
- C. ルールは、検査用のソースネットワークとポートを定義する必要があります。

正解: [\(正解を表示します\)](#)

質問: 43

Cisco Firepowerのインラインタップとインラインタップの違いは何ですか？

- A. インラインモードではSSL復号化を実行できません。
- B. インラインモードは悪意のあるトラフィックをドロップする可能性があります。
- C. インラインタップモードは完全なパケットキャプチャを行います。
- D. インラインタップモードでは、トラフィックのコピーを別のデバイスに送信できます。

正解: [D \(コメントを發表する\)](#)

質問: 44

Cisco FMCで使用できるレポートテンプレートフィールド形式はどれですか。

- A. benchmark chart
- B. bar chart
- C. box lever chart
- D. arrow chart

正解: [\(正解を表示します\)](#)

質問: 45

ネットワークエンジニアは、トラフィックのピーク時のトラフィックの中断を最小限に抑えるという任務を負っています。SNORT検査エンジンが圧倒される場合、この問題を軽減するために何を構成する必要がありますか？

- A. TrustALLアクセス制御ポリシーを設定します。
- B. SNORTエンジンが故障する前にプレフィルタポリシーを有効にします。

- C. 自動アプリケーションバイパスを有効にします。
 - D. IPSインラインリンク状態伝播を有効にする
- 正解: [C \(コメントを發表する\)](#)

質問: 46

ネットワーク管理者は、デバイスの管理されていないすべてのインターフェイスで検査が中断されたことに気づきました。この原因は何ですか？

- A. パッシブインターフェイスがセキュリティゾーンに関連付けられていました。
- B. 非管理インターフェイスに割り当てられた最高のMSSの値が変更されました。
- C. 複数のインラインインターフェイスペアが同じインラインインターフェイスに追加されました。
- D. 非管理インターフェイスに割り当てられた最大MTUの値が変更されました。

正解: [\(正解を表示します\)](#)

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**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/300-710J-mondaishu> **378**問、**30%**ディスカウント、特別な割引コード: **JPNshiken**」

質問: 47

ユーザーがブリッジをルーテッドモードで構成し、デバイスがインターフェイス間でレイヤー2スイッチングを実行できるようにするFirepower機能はどれですか。

- A. IRB
- B. FlexConfig
- C. SGT
- D. BDI

正解: [A \(コメントを發表する\)](#)

質問: 48

企業には、CiscoFMCによって管理される多くのCiscoFTDデバイスがあります。セキュリティモデルでは、分析のためにアクセス制御ルールログを収集する必要があります。セキュリティエンジニアは、CiscoFMCが生成される大量のログを処理できないことを懸念しています。どの構成がこの懸念に対処しますか？

- A. ストレージと分析のためにCiscoFTD接続イベントとセキュリティイベントをCiscoFMCデバイスのクラスタに送信します。
- B. CiscoFTD接続イベントとセキュリティイベントをCiscoFMCに送信し、保存と分析のためにログをSIEMに転送するように設定します。

- C. Cisco FTD接続イベントをSIEMシステムに直接送信し、セキュリティイベントをCiscoFMCからSIEMシステムに転送して保存と分析を行います。
- D. ストレージと分析のためにCiscoFTD接続イベントとセキュリティイベントをSIEMシステムに直接送信します。

正解: [D \(コメントを发表する\)](#)

質問: 49

Cisco FMCで再利用可能でサポートされているオブジェクトの2つのタイプはどれですか。 2つ選択してください。)

- A. IPアドレスとネットワーク、ポート/プロトコルのペア、VLANタグ、セキュリティゾーン、および送信元/送信先の国を表すネットワークベースのオブジェクト
- B. URLカテゴリなどの評判ベースのオブジェクト
- C. レイヤー7アプリケーションプロトコルへのHTTPおよびHTTPS GETリクエストのリンクに役立つ動的キーマッピングオブジェクト。
- D. FQDNマッピングとネットワーク、ポート/プロトコルのペア、VLANタグ、セキュリティゾーン、および送信元/送信先の国を表すネットワークベースのオブジェクト
- E. セキュリティインテリジェンスのフィードとリストを表すレピュテーションベースのオブジェクト、カテゴリとレピュテーションに基づくアプリケーションフィルター、およびファイルリスト

正解: [\(正解を表示します\)](#)

質問: 50

最近の買収により、中堅企業ではネットワーク帯域幅の使用率が高くなっています。ネットワーク運用チームは、ネットワーク帯域幅が増加したため、1つのCiscoFTDアプライアンスの展開をより大容量にスケールアップするよう求められています。この目標を達成するには、どの設計オプションを使用する必要がありますか？

- A. パフォーマンスを向上させるために複数のCisco FTDHAペアを導入する
- B. パフォーマンスを向上させるために、ファイアウォールクラスタリングモードで複数のCiscoFTDアプライアンスを導入します。
- C. VPNロードバランシングを使用して複数のCisco FTDアプライアンスを導入し、パフォーマンスを拡張します。
- D. パフォーマンスを向上させるためにクラスタリングモードで複数のCisco FTDHAペアを導入する

正解: [B \(コメントを发表する\)](#)

質問: 51

エンジニアがネットワークにCiscoFTDを実装し、使用するFirepowerモードを決定しています。組織では、トラフィックセグメンテーションを提供するためにFTDアプライアンス内で複数の仮想Firepowerデバイスを個別に動作させる必要があります。これらの要件をサポートするには、Cisco Firepower ManagementConsoleでどの展開モードを設定する必要がありますか。

- A. マルチインスタンス
- B. 単一展開
- C. 複数の展開
- D. シングルコンテキスト

正解: [A \(コメントを发表する\)](#)

質問: 52

管理者は、CiscoStealthwatchアプライアンスにデータを送信するようにCiscoFirepowerを設定しています。NetFlow_Set_Parametersオブジェクトはすでに作成されていますが、NetFlowはフローコレクターに送信されていません。これを防ぐために何をする必要がありますか？

- A. データをCiscoStealthwatchに送信するためのセキュリティインテリジェンスオブジェクトを作成します
- B. NetFlow_Add_Destinationオブジェクトを構成に追加します
- C. NetFlowサービスを有効にするためのサービス識別子を作成します
- D. NetFlow_Send_Destinationオブジェクトを構成に追加します

正解: [\(正解を表示します\)](#)

質問: 53

ネットワーク管理者は、SIイベントが更新されていないことに気づきました。CiscoFTDデバイスはすべてのSIイベントエントリをロードできず、トラフィックは期待どおりにブロックされていません。この問題を修正するには何をする必要がありますか？

- A. 影響を受けるデバイスをより多くのメモリを提供するデバイスと交換します
- B. 構成をリセットするために、影響を受けるデバイスを再起動します
- C. 適切なトラフィックがブロックされるようにSIイベントエントリを手動で更新します
- D. 影響を受けるデバイスに構成を再デプロイして、追加のメモリがSIモジュールに割り当てられるようにします。

正解: [\(正解を表示します\)](#)

質問: 54

ネットワーク管理者は、CiscoFTDによって検出されたファイルの不明な判定を確認しています。Talosクラウド内のファイルをさらに分析するには、どのマルウェアポリシー構成オプションを選択する必要がありますか？

- A. マルウェア分析
- B. 動的解析
- C. スペロ分析
- D. サンドボックス分析

正解: [\(正解を表示します\)](#)

質問: 55

レポートテンプレートを作成するとき、特定のサブネットのアクティビティのみを表示するように結果を制限するにはどうすればよいですか？

- A. テーブルビューセクションをレポートに追加し、検索フィールドをCIDR形式のネットワークとして定義します。
- B. Firepower Management Centerでカスタム検索を作成し、レポートの各セクションで選択します。
- C. レポートの詳細設定で入力パラメーターを追加し、タイプをネットワーク/IPに設定します。
- D. レポートの各セクションで、X軸としてIPアドレスを選択します。

正解: ([正解を表示します](#))

質問: 56

IT管理者は、ネットワークエンジニアに、ネットワーク内のCiscoFTDアプライアンスの高レベルの要約統計量を提供するように求めています。ビジネスはピークシーズンに近づいているため、ビジネスの稼働時間を維持する必要性が高くなっています。この情報を収集するには、どのレポートタイプを使用する必要がありますか？

- A. SNMPレポート
- B. リスクレポート
- C. マルウェアレポート
- D. 標準レポート

正解: ([正解を表示します](#))

質問: 57

エンジニアはネットワークに冗長性を組み込む必要があり、ファイアウォールの前にある冗長スイッチがダウンした場合でもトラフィックは継続的に流れる必要があります。このタスクを実行するには、何を構成する必要がありますか？

- A. ファイアウォールクラスター上のスパンEtherChannelへのスイッチ上のvPC
- B. ファイアウォールクラスターモードとスイッチの冗長インターフェース
- C. ファイアウォールダスターのインターフェイスモードに切り替わるvPC
- D. ファイアウォールの非クラスターモードとスイッチの冗長インターフェース

正解: ([正解を表示します](#))

質問: 58

エンジニアが、NATIDがACME001でパスワードがCisco388267669のNATデバイスの背後にあるFMCに新しいFTDデバイスを追加しようとしています。これを実現するには、どのコマンドセットを使用する必要がありますか？

- A. マネージャーの追加<FMCIP>登録キー> ACME001を構成します
- B. configure manager add DONTRESOLVE <FMC IP> AMCE001 <登録キー>
- C. configure manager add <FMC IP> ACME001 <登録キー>
- D. configure manager add ACME001 <registration key> <FMC IP>

正解: ([正解を表示します](#))

質問: 59

組織内のユーザーがワークステーションで悪意のあるファイルを開いたため、ネットワークにランサムウェア攻撃が発生しました。サンドボックスシステムでファイルのウイルステストを確実に行うには、Cisco FMC内で何を設定する必要がありますか？

- A. ローカルマルウェア分析
- B. 動的解析
- C. Spere分析
- D. 容量処理

正解: [B \(コメントを發表する\)](#)

質問: 60

エンジニアは、CiscoFMCでコマンドrestoreremote-manager-backup location 2.2.2.2 admin /Volume/home/adminFTD408566513.zipを実行します。リポジトリに接続した後、CiscoFTDデバイスはバックアップファイルを受け入れることができません。この失敗の理由は何ですか？

- A. バックアップファイルが.cfg形式ではありません。
- B. ディレクトリの場所が正しくありません。
- C. 間違ったIPアドレスが使用されています。
- D. バックアップファイルの拡張子が.tarから.zipに変更されました。

正解: [\(正解を表示します\)](#)

質問: 61

エンジニアは、2つの別々のネットワーク上にある営業部門と製品開発部門からのネットワークトラフィックを監視しています。両方の部門のデータプライバシーを維持するには、何を構成する必要がありますか？

- A. 両方の部門にTAPモードで設定された1組のインラインを使用します
- B. 論理トラフィックの分離を維持するためにVLANで802 1Q mimesetトランクインターフェイスを使用する
- C. 両方の部門にパッシブIDSポートを使用する
- D. 各部門に専用のIPSインラインセットを使用して、トラフィックの分離を維持します

正解: [\(正解を表示します\)](#)

有効的な**300-710J**問題集はJPNTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-710J**試験問題集を提供します。JPNTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**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/300-710J-mondaishu> 378問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 62

セキュリティエンジニアが、複数のブランチロケーションのアクセス制御ポリシーを構成しています。これらの場所は共通のルールセットを共有し、各場所でローカルに重要な内部ネットワークサブネットを含むINSIDE_NETと呼ばれるネットワークオブジェクトを利用します。各場所でポリシーの一貫性を維持しながら、該当するルール内でローカルに重要なネットワークサブネットのみを許可する手法はどれですか。

- A. デバイスごとに一意のアクセス制御ポリシーを作成する
- B. ポリシーの継承を利用する
- C. CiscoTalosから更新される動的アクセス制御ポリシーを利用する
- D. INSIDE_NETネットワークオブジェクトとオブジェクトオーバーライドを使用してアクセス制御ポリシーを作成する

正解: ([正解を表示します](#))

有効的な300-710J問題集はJPNTTest.com提供され、300-710J試験に合格することに役に立ちます！JPNTTest.comは今最新300-710J試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで300-710J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/300-710J-mondaishu> 378問、30%ディスカウント、特別な割引コード: **JPNshiken**」