Cisco.300-710J.v2021-08-10.q50

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：	50
バージョン：	v2021-08-10
ページの閲覧量：	576
問題集の閲覧量：	6796

https://www.jpnshiken.com/shiken/Cisco.300-710J.v2021-08-10.q50.html

質問: **1**
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. サンドボックス分析
C. 動的解析
D. スペロ分析
正解: **(**正解を表示します**)**

質問: **2**
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。
正解:
Explanation
Explanation
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_management_center_high_availability.html#id_32288

質問: **3**
Cisco ASA Firepowerモジュールを導入する場合、組織はネットワークに影響を与えずにトラフィックの内容を評価したいと考えています。現在、物理アプライアンス上に同じデバイスの複数のインスタンスを持つように構成されています。組織のニーズを満たす展開モードはどれですか。
A. パッシブタップモニターのみのモード
B. インラインモード
C. インラインタップモニター専用モード
D. パッシブモニター専用モード

正解: **(**正解を表示します**)**

質問: **4**
Cisco FMCがHTTPS証明書に対してサポートする最大ビットサイズはいくつですか？
A. 1024
B. 8192
C. 4096
D. 2048
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/system_configuration.html

質問: **5**
高可用性をサポートする2つの展開タイプはどれですか？ 2つ選択してください。）
A. 透明
B. ルーティング
C. クラスター化
D. シャーシ内マルチインスタンス
E. パブリッククラウドの仮想アプライアンス
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html

質問: **6**
管理者はCiscoASAからCiscoFTDアプライアンスへの移行に取り組んでおり、トラフィックを中断せずにルールをテストする必要があります。移行のこのフェーズでASAルールを設定するには、どのポリシータイプを使用する必要がありますか。
A. アイデンティティ
B. 侵入
C. アクセス制御
D. プレフィルター
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-M

質問: **7**

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. 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
D. 両方の部門にパッシブIDSポートを使用する
正解: **B** (コメントを発表する)

質問: **8**
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. Spere分析
B. 動的解析
C. ローカルマルウェア分析
D. 容量処理
正解: (正解を表示します)

質問: **9**
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. 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。
B. 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。
C. 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。
D. 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。
E. 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。
正解: (正解を表示します)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

質問: **10**
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. 複数の展開
B. シングルコンテキスト
C. 単一展開
D. マルチインスタンス
正解: **(**正解を表示します**)**

質問: **11**
ネットワークエンジニアは、脅威検出を強化するためにサードパーティの脅威フィードをCisco FMCに追加したいと考えています。この目標を達成するには、どのアクションを実行する必要がありますか。
A. STIXとTAXIIを使用して迅速な脅威の封じ込めを有効にする
B. RESTAPIを使用して迅速な脅威の封じ込めを有効にする
C. RESTAPIを使用してThreatIntelligenceDirectorを有効にする
D. STIXおよびTAXIIを使用してThreat IntelligenceDirectorを有効にする
正解: **(**正解を表示します**)**

質問: **12**
ネットワーク管理者は、リモートアクセスVPNユーザーがネットワーク内から到達できないことに気づきました。ルーティングが正しく構成されていると判断されましたが、リターントラフィックはファイアウォールに入っていますが、ファイアウォールから出ていません。この問題の理由は何ですか。
A. 外部NATIPアドレスが構成されていません。
B. 手動のNAT免除ルールがNATテーブルの先頭に存在しません。
C. 外部NATIPアドレスが間違ったインターフェースに一致するように構成されています。
D. オブジェクトNAT免除ルールがNATテーブルの先頭に存在しません。
正解: **D (**コメントを発表する**)**

質問: **13**
パケットキャプチャのトレースオプションを選択する利点は何ですか？
A. オプションは、各パケットの詳細をキャプチャします。
B. このオプションは、キャプチャされるパケットの数を制限します。
C. オプションは、宛先ホストが別のパスを介して応答するかどうかを示しました。
D. オプションは、パケットがドロップされたか成功したかを示します。
正解: **(**正解を表示します**)**

質問: **14**

Cisco FTDソフトウェアでは、アプライアンスを通過するトラフィックをパッシブに受信するように設定する必要があるインターフェイスモードはどれですか。
A. IPSのみ
B. タップ
C. ファイアウォール
D. ERSPAN
正解: **(**正解を表示します**)**

質問: **15**
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. 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。
B. ルールアクションを信頼から変更して許可する
C. 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
D. ルール内で選択したアプリケーションを変更します
正解: **(**正解を表示します**)**

質問: **16**
ネットワーク管理者は懸念しています ユーザーのマシンに影響を与えるマルウェアファイルが多数あります。この懸念に対処するには、Cisco FMCのアクセス制御ポリシー内で何を行う必要がありますか？
A. ファイルポリシーを作成し、アクセス制御ポリシーを許可するように設定します。
B. 侵入ポリシーを作成し、アクセス制御ポリシーをブロックに設定します。
C. ファイルポリシーを作成し、アクセス制御ポリシーをブロックに設定します。
D. 侵入ポリシーを作成し、アクセス制御ポリシーを許可するように設定します。
正解: **(**正解を表示します**)**

質問: **17**

エンジニアが、Webサーバーに接続できないデバイスのトラブルシューティングを行っています。接続は、Cisco FTD内部インターフェイスから開始され、9443の非標準ポートを介して10.0.1.100に到達しようとしています。エンジニアが接続を試行しているホストは、IPアドレス10.20.10.20にあります。ネットワーク上のパケットに何が起こっているかを判断するために、エンジニアはFTDパケットキャプチャツールを使用することにしました。この問題のトラブルシューティングに必要な情報を収集するには、どのキャプチャ構成を使用する必要がありますか。

A）

B）

C）

D）

A. オプションB

B. オプションC

C. オプションA

D. オプションD

正解: **(**正解を表示します**)**

質問: **18**

HTTP警告ページを表示するCisco Firepowerルールアクションはどれですか。

A. モニター

B. ブロック

C. インタラクティブブロック

D. 警告付きで許可

正解: **C (**コメントを発表する**)**

Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

質問: **19**

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: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

質問: **20**

エンジニアは、ファイル ポリシー構成をセキュリティ ゾーンまたはトンネル ゾーンに展開するアクセス コントロール ルールを構成し、デバイスを再起動します。再開の理由は？
A. アクセス コントロール ルールのソースまたは宛先セキュリティ ゾーンは、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致します。
B. ルールのソース トンネル ゾーンが、宛先ポリシーのトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
C. ルールのソース トンネル ゾーンが、ソース ポリシーのトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
D. ソース トンネル ゾーンのソースまたは宛先セキュリティ ゾーンが、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致しません。
正解: **(**正解を表示します**)**

質問: **21**
Cisco Firepower Management Centerはいくつのレポートテンプレートをサポートしていますか？
A. 20
B. 10
C. 5
D. 無制限
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Working_with_Reports.html

質問: **22**
エンジニアは、アプリケーションの使用状況を毎月自動的に表示し、その情報を管理者に送信するように求められました。このタスクを実行するには、どのメカニズムを使用する必要がありますか？
A. reports
B. context explorer
C. event viewer
D. dashboards
正解: **(**正解を表示します**)**

質問: **23**
エンジニアは、Cisco FMCを使用して、ネットワーク経由で送信されるファイルがマルウェアであるかどうかを判断する必要があります。このファイルルックアップを実現するには、どの2つの構成を実行する必要がありますか？ （2つ選択してください。）
A. Cisco FMCは、Cisco AMP forEndpointsサービスに接続する必要があります。

B. サンドボックス化のためにCiscoFMCはCiscoThreatGridサービスに直接接続する必要があります。
C. Cisco FMCには、マルウェアルックアップ用のファイル検査ポリシーを含める必要があります。
D. CiscoFMCはFireAMPクラウドに接続する必要があります。
E. CiscoFMCにはSSL復号化ポリシーを含める必要があります。
正解: **A,C** (コメントを発表する)

質問: **24**
管理対象デバイスをインラインで展開するための最小要件は何ですか？
A. インラインインターフェイス、セキュリティゾーン、MTU、モード
B. パッシブインターフェイス、MTU、モード
C. インラインインターフェイス、MTU、モード
D. パッシブインターフェイス、セキュリティゾーン、MTU、モード
正解: (正解を表示します)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config- guide-v65/ips_device_deployments_and_configuration.html

質問: **25**
ネットワークエンジニアがCiscoAMP for Endpointsコンソールにログインし、識別されたSHA-256ハッシュに対する悪意のある判定を確認します。この脅威を軽減するには、どの構成が必要ですか？
A. 感染したエンドポイントでパーソナルファイアウォールを有効にします。
B. 感染したエンドポイントからのハッシュをネットワークブロックリストに追加します。
C. 正規表現を使用して悪意のあるファイルをブロックします。
D. ハッシュを単純なカスタム削除リストに追加します。
正解: (正解を表示します)

質問: **26**
エンジニアが新しいFirepower展開をセットアップし、実装を開始するためのデフォルトのFMCポリシーを検討しています。最初の試用段階で、組織は、ネットワークトラフィックの大部分が通過できるようにしながら、いくつかの一般的なSnortルールをテストしたいと考えています。利用される？
A. 最大検出
B. 接続を介したセキュリティ
C. バランスの取れたセキュリティと接続性
D. セキュリティを介した接続
正解: **C** (コメントを発表する)
Explanation

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusio

質問: **27**
Cisco Firepower Threat Defenseで有効なルーティングオプションはどれですか？ （2つ選択してください。）
A. BGPv6
B. 複数のインターフェイス間で最大3つの等コストパスを備えたECMP
C. 単一インターフェイス全体で最大3つの等コストパスを備えたECMP
D. トランスペアレントファイアウォールモードのBGPv4
E. ノンストップフォワーディングを使用するBGPv4
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

質問: **28**
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. CiscoTalosから更新される動的ACPを利用する
C. ポリシーの継承を利用する
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: **29**
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. すべてのプロトコルを同じ方法で表す
D. 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。
正解: **(**正解を表示します**)**

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html

質問: **30**
エンジニアは、Cisco FMC を使用して、ネットワーク経由で送信されているファイルがマルウェアかどうかを判断することを任されています。このファイル検索を実行するには、どの 2 つの構成タスクを実行する必要がありますか? (2つ選んでください)。
A. Cisco FMC に SSL 復号化ポリシーを含める必要があります。
B. Cisco FMC は FireAMP クラウドに接続する必要があります。
C. Cisco FMC は、Cisco AMP for Endpoints サービスに接続する必要があります。
D. Cisco FMC は、サンドボックス化のために Cisco ThreatGrid サービスに直接接続する必要があります。
E. Cisco FMC は、マルウェア ルックアップ用のファイル インスペクション ポリシーを含める必要があります。
正解: **C,E** (コメントを発表する)

質問: **31**
組織のCEOからのネットワークトラフィックのコイニングは決して否定されてはなりません。展開エンジニアがすべてのトラフィックを許可するルールを作成することを許可されていない場合、どのアクセス制御ポリシー構成オプションを使用する必要がありますか?
A. CEOの信頼ポリシーを構成します。
B. ファイアウォールバイパスを構成します。
C. CEO専用のNATポリシーを作成します。
D. 侵入ポリシーをセキュリティからバランスに変更します。
正解: (正解を表示します)

質問: **32**
FTDを構成する際、ネットワークエンジニアは、アプライアンスを通過するトラフィックがルーティングやVLANの書き換えを必要としないことを確認したいと考えています。このタスクを実行するには、エンジニアはどのインターフェイスモードを実装する必要がありますか?

A. 透明
B. インラインセット
C. パッシブ
D. インラインタップ
正解: **A** (コメントを発表する)

質問: **33**
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. /sf/etc/DCEALERT.MIB
C. /etc/sf/DCEALERT.MIB
D. system/etc/DCEALERT.MIB
正解: (正解を表示します)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-Responses.pdf

質問: **34**
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。
B. インラインモードではSSL復号化を実行できません。
C. 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。
D. 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。
正解: **C** (コメントを発表する)

質問: **35**
AMPがファイルをマルウェアとして識別したことをCisco Threat Responseが通知した場合、どのアクションを実行する必要がありますか？
A. 調査結果を外部の脅威分析エンジンに転送する。
B. テクニカルサポートのためにスナップショットをシスコに送信します。
C. Cisco Threat Responseがマルウェアを自動的にブロックするのを待ちます。
D. 悪意のあるファイルをブロックリストに追加します。
正解: **D** (コメントを発表する)

質問: **36**
Cisco FTD統合ルーティングおよびブリッジングでは、ブリッジグループはルーティングされたインターフェイスとの通信にどのインターフェイスを使用しますか。
A. 仮想スイッチ
B. ブリッジグループメンバー

C. 仮想ブリッジ
D. サブインターフェース
正解: **C** (コメントを発表する)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transp

質問: **37**
どのオブジェクトタイプがオブジェクトのオーバーライドをサポートしていますか？
A. 時間範囲
B. セキュリティグループタグ
C. ネットワークオブジェクト
D. DNSサーバーグループ
正解: (正解を表示します)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

質問: **38**
ClientHelloメッセージの特別な処理を制御するために使用されるCLIコマンドはどれですか？
A. system support ssl-client-hello-display
B. system support ssl-client-hello-enabled
C. system support ssl-client-hello-force-reset
D. system support ssl-client-hello-tuning
正解: (正解を表示します)

質問: **39**
組織にはクライアントからサーバーを保護するためのコンプライアンス要件がありますが、クライアントとサーバーはすべて同じレイヤー3ネットワーク上にあります。クライアントまたはサーバーのIPサブネットを再アドレス指定せずに、セグメンテーションはどのように実現されますか？」
A. 同じサブネットにとどまりながら、サーバーのIPアドレスを変更します
B. クライアントとサーバーの間にファイアウォールを透過モードで展開します。
C. クライアントとサーバー間にルーティングモードでファイアウォールを展開します
D. 同じサブネット上にとどまりながら、クライアントのIPアドレスを変更します。
正解: (正解を表示します)

質問: **40**

エンジニアは、CiscoFMCを使用して新しいアクセスコントロールポリシーを構築しています。ポリシーは、一意のIPSポリシーとログルールの一致を検査する必要があります。これらの要件を満たすには、どのアクションを実行する必要がありますか？
A. デフォルトのIPSポリシーを無効にし、ルールごとのログを有効にします。
B. IPSポリシーを構成し、グローバルロギングを有効にします。
C. デフォルトのIPSポリシーを無効にし、グローバルロギングを有効にします。
D. IPSポリシーを構成し、ルールごとのロギングを有効にします。
正解: **(**正解を表示します**)**

質問: **41**
組織はIPS機能なしでCiscoFirepowerを実装しており、トラフィックの検査を有効にしたいと考えています。彼らは、プロトコルの異常を検出し、Snortルールセットを利用して悪意のある動作を検出できる必要があります。これはどのように達成されますか？
A. 侵入ポリシーを変更して、検査するイベントの最小重大度を決定します。
B. アクセス制御ポリシーを変更して、対象のトラフィックをエンジンにリダイレクトします
C. 検査のためにパケットを処理するようにネットワーク分析ポリシーを変更します
D. ネットワーク検出ポリシーを変更して、検査する新しいホストを検出します
正解: **(**正解を表示します**)**

質問: **42**
ルーティングされたインターフェイスを構成するときに必要な2つのインターフェイス設定のうち、どのCisco Firepower Threat Defenseですか。 2つ選択してください。）
A. 冗長インターフェース
B. EtherChannel
C. スピード
D. メディアタイプ
E. デュプレックス
正解: **(**正解を表示します**)**
Explanation
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

質問: **43**
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. 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。

B. 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
C. 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
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、VXLAN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. URLカテゴリなどの評判ベースのオブジェクト
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-00000414

質問: **44**
Cisco AMP for Endpointsの2つの機能で、アップロードされたファイルをブロックできますか？ （2つ選択してください。）
A. アプリケーションのブロック
B. 簡単なカスタム検出
C. アプリケーションのホワイトリスト
D. ファイルリポジトリ
E. 除外
正解: **(**正解を表示します**)**

質問: **45**
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. NetFlow_Send_Destinationオブジェクトを構成に追加します
B. NetFlow_Add_Destinationオブジェクトを構成に追加します
C. 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
D. 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
正解: **C (**コメントを発表する**)**

質問: **46**
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。デバイスを通過す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. 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。
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. CiscoFirepowerでルーティングを有効にします
D. ブリッジグループを透過モードで構成します。
正解: **(**正解を表示します**)**

質問: **47**
オブジェクト オーバーライドをサポートするオブジェクト タイプはどれですか。
A. DNSサーバーグループ
B. セキュリティグループタグ
C. 時間範囲
D. ネットワーク オブジェクト
正解: **(**正解を表示します**)**

質問: **48**
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適用される前に有効化されていませんでした
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.cfg形式ではありません。
正解: **B (**コメントを発表する**)**

質問: **49**
管理者がSSHを使用してデータセンターのスイッチにリモートログインしようとしていますが、接続できません。管理者は、トラフィックがファイアウォールに到達していることをどのように確認しますか？
A. ファイアウォールでパケットトレーサーを実行する。
B. 管理者のPCでWiresharkを実行する
C. ファイアウォールでパケットキャプチャを実行する。

D. 別のワークステーションからアクセスを試みることによって。
正解: **(**正解を表示します**)**

質問: **50**
FTDでトラブルシューティングファイルを生成するには、どのコマンドを実行する必要がありますか？
A. システムサポートビューファイル
B. sudo sf_troubleshoot.pl
C. システムはすべてトラブルシューティングを生成します
D. 技術サポートを表示する
正解: **(**正解を表示します**)**
Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote- SourceFire-00.html