Cisco.300-710J.v2021-08-21.q41

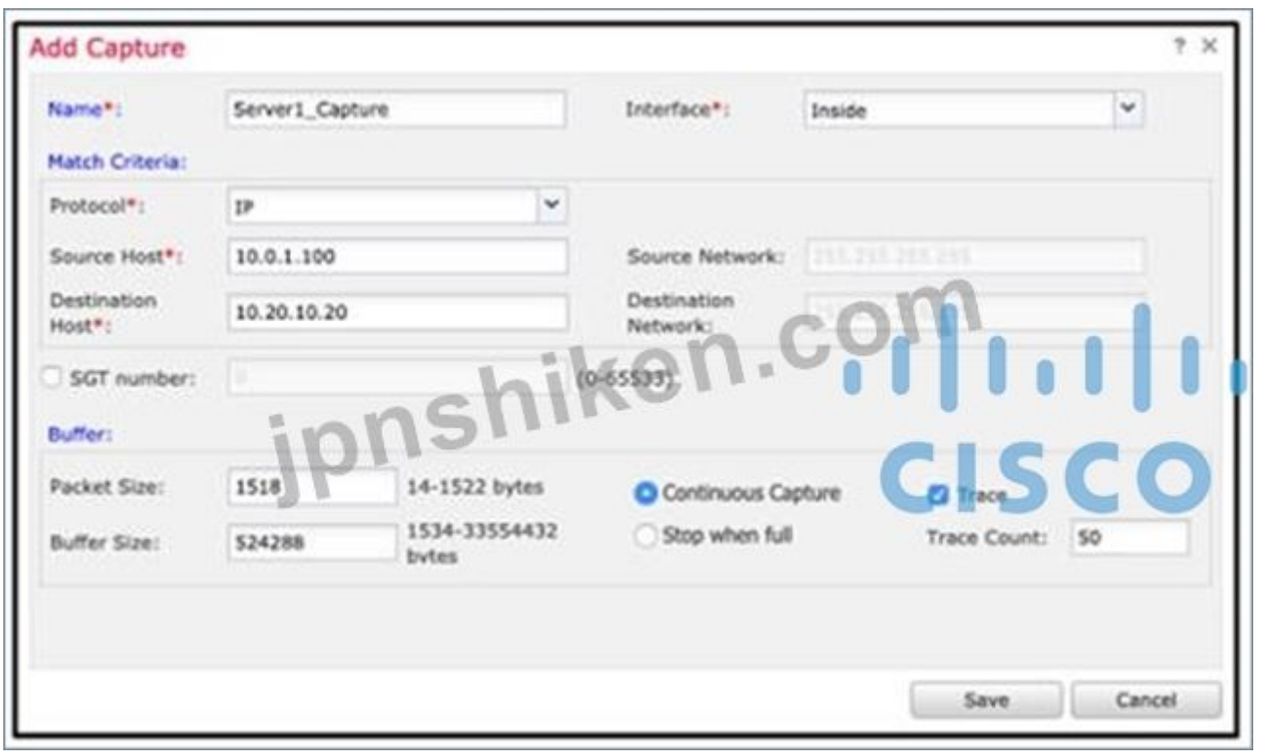
試験コード：	300-710J
試験名称：	Securing Networks with Cisco Firepower (300-710日本語版)
認証ベンダー：	Cisco
無料問題の数：	41
バージョン：	v2021-08-21
ページの閲覧量：	584
問題集の閲覧量：	3831

https://www.jpnshiken.com/shiken/Cisco.300-710J.v2021-08-21.q41.html

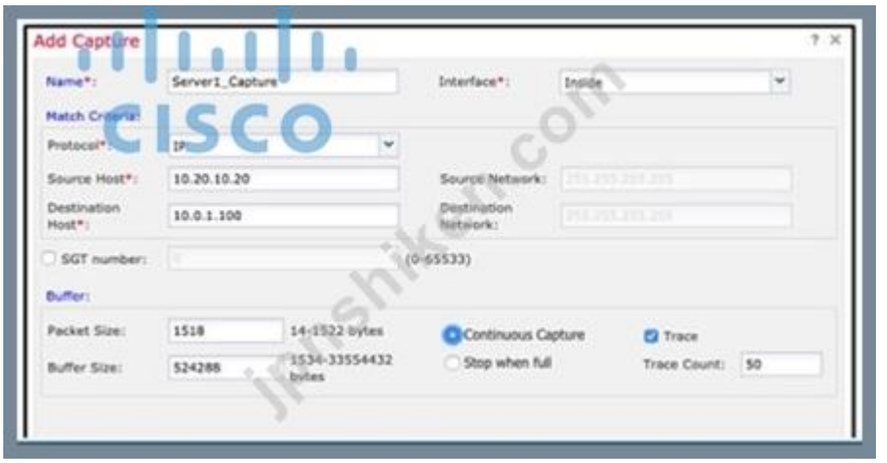
質問: **1**

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。

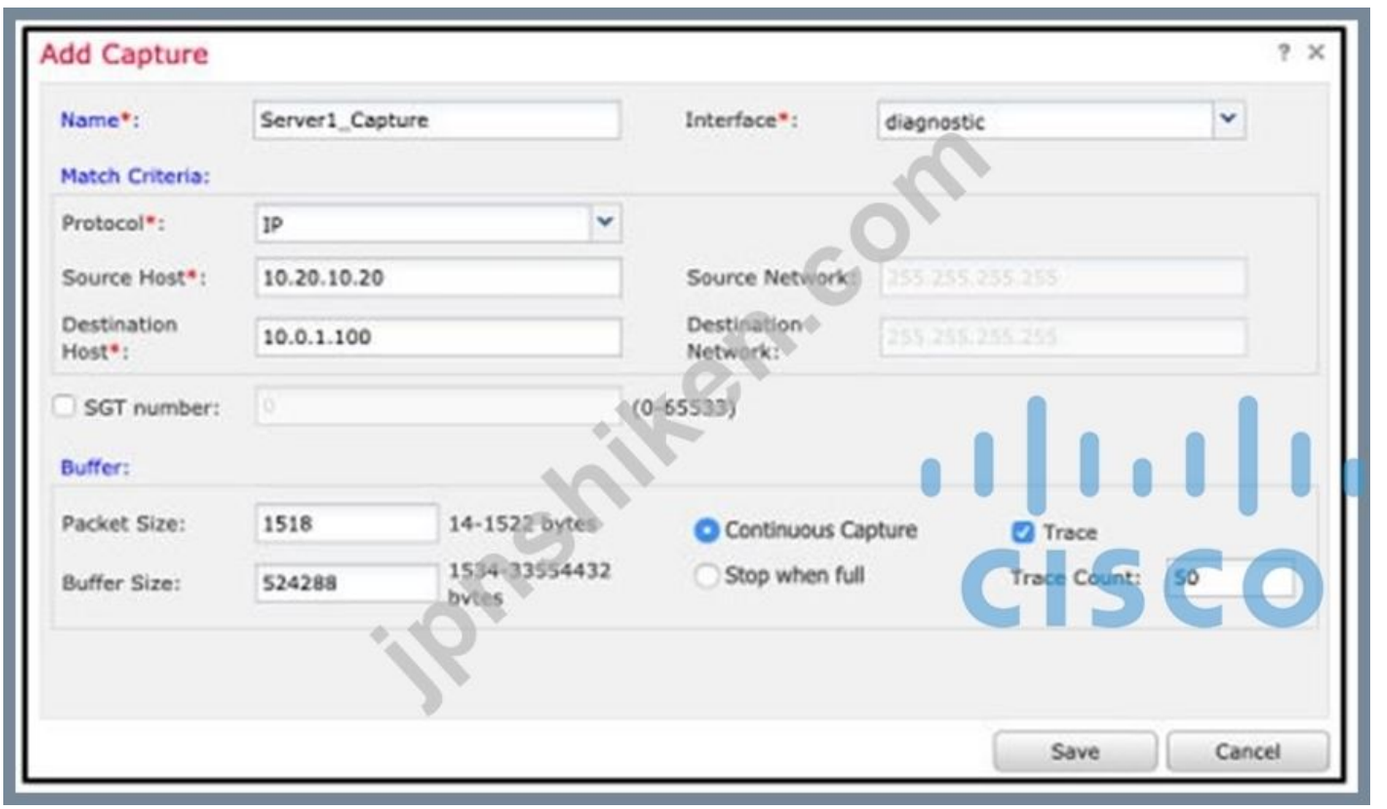
A）



B）


Add Capture
Name*: Server1_Capture
Interface*: Inside
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network:
Destination Host*: 10.0.1.100
Destination Network:
SGT number:
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50

C)


Add Capture
Name*: Server1_Capture
Interface*: diagnostic
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255
SGT number: 0
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50
Save
Cancel

D)

A. オプションD
B. オプションA
C. オプションB
D. オプションC
正解: **(**正解を表示します**)**

質問: **2**
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つの構成タスクを実行する必要がありますか？ （2つ選択してください。）
A. CiscoFMCにはSSL復号化ポリシーを含める必要があります。
B. Cisco FMCは、Cisco AMP forEndpointsサービスに接続する必要があります。
C. 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。
D. CiscoFMCはFireAMPクラウドに接続する必要があります。
E. 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。
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/Reference_a_wrapper_Chapter_topic_here.html#ID-2193-00000296

質問: **3**
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. 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。
B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **4**
エンジニアが2番目のCiscoFMCをスタンバイデバイスとして設定していますが、アクティブユニットに登録できません。この問題の原因は何ですか？
A. プライマリFMCには、現在デバイスが接続されています。
B. CiscoFMCデバイスで実行されているコードバージョンが異なります
C. 購入したライセンスには高可用性が含まれていません
D. 2つのデバイス間の帯域幅はわずか10Mbpsです。
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html

質問: **5**
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. context explorer
B. event viewer
C. reports
D. dashboards
正解: **C (**コメントを発表する**)**

質問: **6**
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. 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。
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. 悪意のあるファイルをブロックリストに追加します。
D. 調査結果を外部の脅威分析エンジンに転送する。
正解: **C (**コメントを発表する**)**

質問: **7**
Cisco Firepower Management Center CLIでサポートされているコマンドラインモードはどれですか。
A. 管理者

B. 特権
C. ユーザー
D. 構成
正解: **(**正解を表示します**)**

質問: **8**
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. 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。
B. 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。
C. 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。
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: **B,D (**コメントを発表する**)**

質問: **9**
一定期間に受信するイベントの数を減らすために使用されるCisco Firepower機能はどれですか。
A. レート制限
B. 一時停止
C. 相関
D. しきい値処理
正解: **(**正解を表示します**)**

質問: **10**
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. 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
B. 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。
C. 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。
D. 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
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/fdm/fptd-fdm-config-guide-640/fptd-fdm-ravpn.html

質問: **11**
しきい値設定を構成できる2つの場所はどれですか。 （2つ選択してください。）
A. 侵入ポリシーごとにグローバルに
B. 各IPSルール
C. 各アクセス制御ルールについて
D. グローバルに、ネットワーク分析ポリシー内
E. プリプロセッサごと、ネットワーク分析ポリシー内
正解: **A,B (**コメントを発表する**)**

質問: **12**
ネットワークエンジニアは、別のIPサブネットを作成せずに、トラフィック検査のためにFTDデバイスを介してユーザーセグメントを拡張しています。これは、ルーティングモードのFTDデバイスでどのように実現されますか？
A. ARPを活用してトラフィックをファイアウォール経由で転送する
B. インラインセットインターフェイスを割り当てる
C. BVIを使用して、ユーザーセグメントと同じサブネットにBVIIPアドレスを作成します
D. プレフィルタールールを活用してプロトコル検査をバイパスする
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

質問: **13**
最近の夏時間の変更により、システムログには、リアルタイムより1時間遅れて発生したアクティビティが表示されます。この問題を解決するには、どのアクションを実行する必要がありますか？
A. NTPを使用するようにシステムクロック設定を構成します
B. CiscoFMCで時間を手動で正しい時間に調整します。
C. すべての管理対象デバイスで時間を手動で正しい時間に調整します
D. 夏時間をチェックしてNTPを使用するようにシステム時刻設定を構成します
正解: **(**正解を表示します**)**

質問: **14**
FTD LINAエンジンはどの2つのパケットキャプチャをサポートしていますか？ （2つ選択してください。）
A. アプリケーションID
B. プロトコル
C. レイヤー7ネットワークID
D. ソースIP

E. 動的なファイアウォールのインポート
正解: **(**正解を表示します**)**

質問: **15**
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. モニター
B. 分析
C. リセット付きブロック
D. すべてをブロック
E. 発見
正解: **(**正解を表示します**)**

質問: **16**
エンジニアは、組織のプライマリCiscoFMCにディザスタリカバリを提供する任務を負っています。プライマリCiscoFMCに障害が発生した場合に、元の企業ポリシーのコピーを確実に使用できるようにするには、プライマリおよびセカンダリCiscoFMCで何を行う必要がありますか。
A. プライマリとセカンダリの両方のCiscoFMCでハイアベイラビリティを設定します
B. プライマリおよびセカンダリCisco FMCデバイスを、長さが10メートル以下のカテゴリ6ケーブルで接続します。
C. アクティブなCiscoFMCデバイスをスタンバイデバイスと同じ信頼できる管理ネットワークに配置します
D. プライマリデバイスに障害が発生した場合、プライマリCiscoFMCバックアップ設定をセカンダリCiscoFMCデバイスに復元します
正解: **A (**コメントを発表する**)**
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

質問: **17**
Cisco AMP for Networksの導入で、クラウドに到達できない場合に返される処理はどれですか。
A. きれい

B. 切断された
C. 利用できません
B不明
正解: **C** (コメントを発表する)

質問: **18**
ネットワークエンジニアは、データセンターのFTDアプライアンスを通過する企業アプリケーションからランダムに切断されたユーザーのレポートを受信しています。ネットワーク監視ツールは、FTDアプライアンスの使用率が総容量の90%を超えてピークに達していることを示しています。この問題をさらに分析するには、何をする必要がありますか？
A. パケットエクスポート機能を使用してデータを外付けドライブに保存します
B. パケットキャプチャ機能を使用して、リアルタイムのネットワークトラフィックを収集します
C. トラフィックポリシー分析にパケットトレーサー機能を使用する
D. パケット分析機能を使用してネットワークデータをキャプチャします
正解: (正解を表示します)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

質問: **19**
ネットワーク上のトラフィック量が増加しており、コンプライアンス上の理由から、管理者は暗号化されたトラフィックを可視化する必要があります。TLSのSSL復号化を有効にしてこの可視性を実現した結果はどうなりますか？
A. 証明書のピン留めが強制されていない場合は失敗します
B. プライバシー規制の対象ではありません
C. 企業が管理する証明書の必要性を促します
D. パフォーマンスへの影響は最小限です
正解: (正解を表示します)

質問: **20**
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. パブリッククラウドの仮想アプライアンス
B. ルーティング
C. 透明
D. シャーシ内マルチインスタンス
E. クラスター化
正解: (正解を表示します)

質問: **21**

組織は、現在のファイアウォールを置き換えるために2つの新しいCisco FTDデバイスをセットアップしており、ネットワークのダウンタイムは発生しません。セットアッププロセス中に、2つのデバイス間の同期が失敗します。この問題を解決するには、どのようなアクションが必要ですか。
A. 両方のデバイスのポートチャネル番号が同じであることを確認します
B. 両方のデバイスが同じソフトウェアバージョンを実行していることを確認します
C. 両方のデバイスが同じタイプのインターフェースで構成されていることを確認します
D. 両方のデバイスのフラッシュメモリサイズが同じであることを確認します
正解: **B** (コメントを発表する)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/ firepower_threat_defense_high_availability.html#Cisco_Reference.dita_cc8821d8-a5a5-49c0-97fddc9b6f7dbad2

質問: **22**
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. 管理者のPCでWiresharkを実行する
B. ファイアウォールでパケットキャプチャを実行する。
C. ファイアウォールでパケットトレーサーを実行する。
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: **C** (コメントを発表する)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc16

質問: **23**
インターフェイスにヒットするすべてのパケットをキャプチャするには、Cisco FTD CLIでどのコマンドを使用する必要がありますか？
A. キャプチャ
B. コアダンプパケットエンジンを有効にする
C. WORDをキャプチャする
D. キャプチャトラフィック
正解: (正解を表示します)

質問: **24**
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. 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。

B. 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。
C. 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。
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が利用できるので、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。
E. 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。
正解: **(**正解を表示します**)**

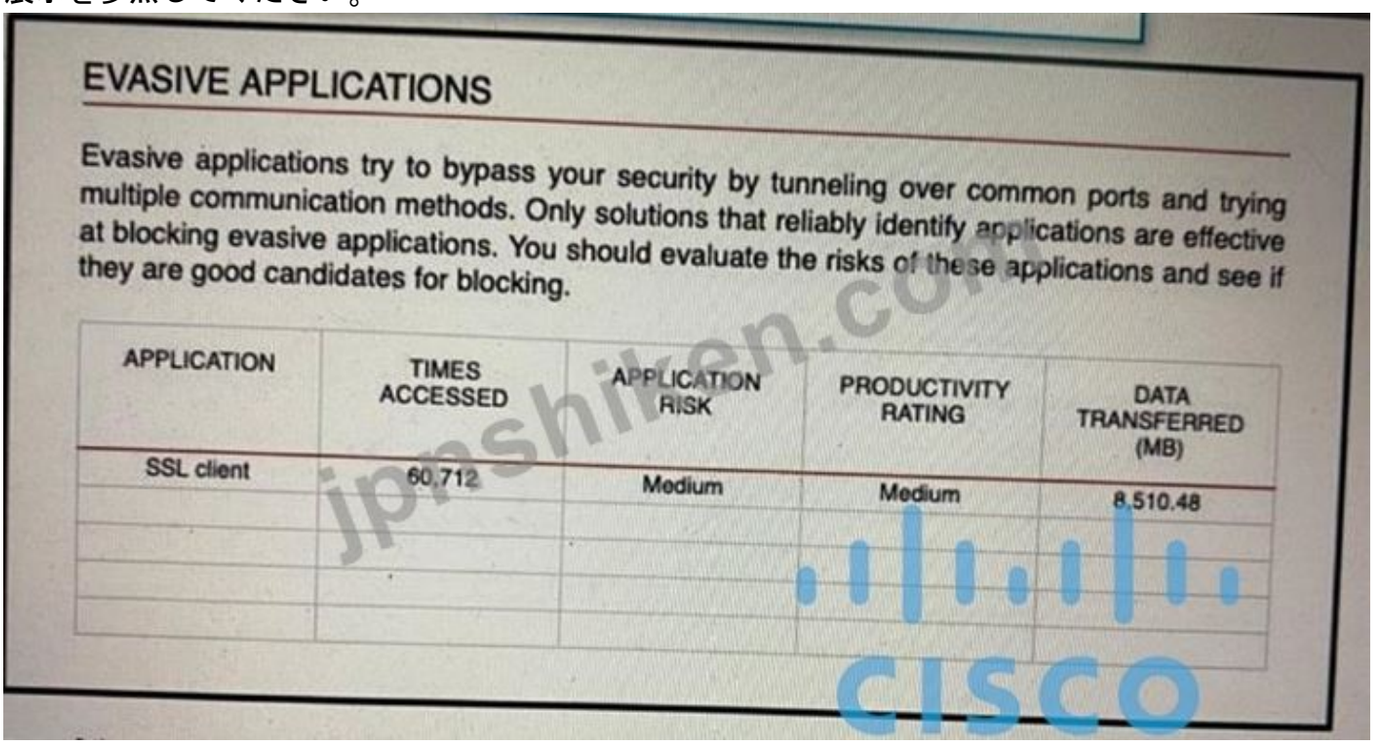
質問: **25**
2つのCisco FTDデバイス間で高可用性が機能するために必要な2つの条件はどれですか。
（2つ選択してください。）
A. ユニットは同じバージョンである必要があります
B. 両方のデバイスは、FMC内で構成されている場合、同じドメインにある必要がある別のグループの一部になることができます。
C. ユニットは、ファイアウォールルーテッドモードでのみ構成する必要があります。
D. ユニットが同じシリーズの一部である場合、ユニットは異なるモデルでなければなりません。
E. ユニットは同じモデルでなければなりません。
正解: **(**正解を表示します**)**

質問: **26**
Cisco FMCデータベースパージの動作は何ですか。
A. 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。
B. データはデバイスから復元できます。
C. 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。
D. 適切なプロセスが再起動されます。
正解: **(**正解を表示します**)**

質問: **27**
ネットワーク管理者は、ユーザーがファイルサーバーに接続し、マルウェアファイルをダウンロードしたことを発見しました。Cisc FMCはマルウェアイベントのアラートを生成しましたが、ユーザーは接続を維持しました。この問題を解決するには、CiscoFMC内のどのCiscoAPMファイルルールアクションを設定する必要がありますか。
A. マルウェアクラウドルックアップ
B. ローカルマルウェア分析
C. ファイルを検出する
D. 接続をリセット
正解: **(**正解を表示します**)**

質問: **28**
CiscoFTDで有効な2つの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. 透過ファイアウォールモードのBGPv4
B. BGPv6
C. ノンストップ転送のBGPv4
D. 複数のインターフェイスにまたがる最大3つの等しいコストパスを備えたECMP
E. 単一のインターフェイス全体で最大3つの等しいコストパスを持つECMP
正解: **(**正解を表示します**)**

質問: **29**
展示を参照してください。



管理者は、Cisco Firepowerのレポート機能のいくつかを調べており、ネットワークリスクレポートのこのセクションに、クラウドが回避に使用される多くのSSLアクティビティが示されていることに気づきました。このリスクを軽減するアクションはどれですか？
A. SSL復号化を使用してパケットを分析します。
B. 暗号化されたトラフィック分析を使用して攻撃を検出する
C. Cisco AMP forEndpointsを使用してすべてのSSL接続をブロックします
D. CiscoTetrationを使用してサーバーへのSSL接続を追跡します。
正解: **(**正解を表示します**)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ssl-decryption.html

質問: **30**

Which two packet captures does the FTD LINA engine support?
A. Layer 7 network ID
B. source IP
C. protocol
D. dynamic firewall importing
E. application ID
正解: (正解を表示します)

質問: **31**
ネットワーク上のトラフィック量が増加しており、コンプライアンス上の理由から、管理者は暗号化されたトラフィックを可視化する必要があります。TLSのSSL復号化を有効にしてこの可視性を実現した結果はどうなりますか？
A. パフォーマンスへの影響は最小限です
B. プライバシー規制の対象ではありません
C. 企業が管理する証明書の必要性を促します
D. 証明書のピン留めが強制されていない場合は失敗します
正解: (正解を表示します)

質問: **32**
組織は、マルウェアが現在既知の悪い評判を持っていないWebサイトからダウンロードされたことに気づきました。この問題は、可能な限り迅速に、影響を最小限に抑えて、グローバルにどのように対処されますか？
A. アウトバウンドWebアクセスを拒否する
B. エンドポイントを分離する
C. CiscoTalosはポリシーを自動的に更新します。
D. ポリシーにURLオブジェクトを作成して、Webサイトをブロックします
正解: (正解を表示します)

質問: **33**
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. ERSPAN

B. IPSのみ
C. ファイアウォール
D. タップ
正解: (正解を表示します)
Reference:
v64/interface_overview_for_firepower_threat_defense.html

質問: **34**
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. 侵入ルールのローカルインポート
B. Ciscoジオロケーションデータベース
C. メジャーアップグレードのローカルインポート
D. マイナーアップグレード
正解: (正解を表示します)

質問: **35**
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. サブインターフェース
B. 仮想ブリッジ
C. ブリッジグループメンバー
D. 仮想スイッチ
正解: (正解を表示します)

質問: **36**
組織では、インターネットに送信されるリンクで多くのトラフィックの輻輳が発生しています。企業を離れる前にインターネットに送信されるすべてのトラフィックを処理するCiscoFirepowerデバイスがあります。正当なビジネストラフィックが目的地に到達するように、輻輳はどのように緩和されますか？
A. QoSポリシーのレート制限高帯域幅アプリケーションを作成します
B. アプリケーション対応の帯域幅制限にWCCPを使用するflexconfigポリシーを作成します
C. ビジネスアプリケーションへの直接トンネルが確立されるようにVPNポリシーを作成します
D. CiscoFirepowerデバイスが多くのアドレスを変換する必要がないようにNATポリシーを作成します
正解: (正解を表示します)

質問: **37**
Cisco FMCpxGridと統合するためにCiscoISEで必要なライセンスタイプはどれですか。
A. モビリティ

B. プラス
C. ベース
D. 頂点
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_0111.html#concept_DE1C38E055794B198ED352D1528B5182

質問: **38**
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. 簡単なカスタム検出
B. アプリケーションのホワイトリスト
C. アプリケーションのブロック
D. 除外
E. ファイルリポジトリ
正解: **A,C (**コメントを発表する**)**

質問: **39**
Cisco Firepowerシステムでアクセスコントロールポリシーが機能するのはどの2つの方法ですか？（2つ選択してください。）
A. 設定の変更が導入されると、トラフィック検査が一時的に中断される可能性があります。
B. ファイルポリシーは、関連する変数セットを使用して侵入防止を実行します。
C. システムは侵入検査を実行した後、ファイル検査を実行します。
D. システムは、信頼できるトラフィックの予備検査を実行して、信頼できるパラメータと一致することを検証します。
E. セキュリティインテリジェンスデータに基づいてトラフィックをブロックできます。
正解: **A,E (**コメントを発表する**)**

質問: **40**
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. 無制限
B. 5
C. 20
D. 10
正解: **(**正解を表示します**)**

質問: **41**
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 "show tech" file for the device in question
C. A "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC
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/troubleshooting_the_system.html