Cisco.300-710J.v2026-09-30.q165

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：	165
バージョン：	v2026-09-30
ページの閲覧量：	102
問題集の閲覧量：	1682

https://www.jpnshiken.com/shiken/Cisco.300-710J.v2026-09-30.q165.html

質問: **1**
エンジニアが新しいCisco Secure Firewallを導入しています。このファイアウォールは、以下の3つのサブネット間のトラフィックを遮断する必要があります。
* LAN 192.168.101.0724
* DMZ 192.168 200.0/24
*WAN 10.0.0.0/30
エンジニアはどのファイアウォールモードを実装する必要があるか？
A. 透明
B. ネットワーク
C. ルーティング済み
D. ゲートウェイ
正解: (正解を表示します)
To filter traffic between multiple subnets, the engineer must implement the firewall in routed mode. In routed mode, the firewall operates as a Layer 3 device, capable of routing traffic between different IP subnets. This mode is appropriate for filtering traffic between LAN, DMZ, and WAN subnets.
Steps to configure routed mode:
Access the firewall ' s management interface.
Configure interfaces for each subnet (LAN, DMZ, WAN) with appropriate IP addresses and network masks.
Define security zones and apply access control policies to filter traffic as required.
This ensures that the firewall can inspect and route traffic between the different subnets, providing the necessary security and control.
References:Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Routed Mode Configuration.

質問: **2**
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. 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
B. 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
C. 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
D. CiscoFMCで時間を手動で正しい時間に調整します。
正解: (正解を表示します)

質問: **3**

管理者は、標準の営業時間外に内部ホストから 10 MB を超えるデータ転送が開始されたときに通知電子メールを送信するように Cisco FMC 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 Cisco FMC 機能を設定する必要がありますか?
A. アプリケーション検出器
B. 侵入ポリシー
C. 相関ポリシー
D. ファイルおよびマルウェア ポリシー
正解: **(**正解を表示します**)**

質問: **4**
ネットワーク エンジニアは、Cisco Secure Firewall Management Center で管理される 2 台の Cisco Secure Firewall Threat Defense デバイスを展開しています。インターネット アクセスはビジネスにとって最優先事項であるため、2 つの異なる ISP からインターネット回線に投資しています。顧客からの要件は、ISP のいずれかがダウンした場合でも、ユーザーのオーブンにインターネット アクセスが利用可能である必要があるということです。この要件を満たすために展開する必要がある 2 つの機能はどれですか? (2 つ選択してください。)
A. EtherChannel インターフェイス
B. ルート トラッキング
C. SLA モニタ
D. 冗長インターフェイス
E. BGP
正解: **B,C (**コメントを発表する**)**
To ensure high availability of internet access when deploying a pair of Cisco Secure Firewall Threat Defense (FTD) devices managed by Cisco Secure Firewall Management Center (FMC), the following features must be deployed:
Route Tracking:This feature monitors the reachability of a specified target (such as an external IP address) through the configured routes. If the route to the target is lost, the FTD can dynamically adjust the routing to use an alternate path, ensuring continuous internet access.
SLA Monitor:Service Level Agreement (SLA) monitoring works alongside route tracking to continuously verify the status and performance of the internet links. If the SLA for one of the ISP links fails (indicating the link is down or underperforming), the FTD can switch traffic to the secondary ISP link.
Steps to configure:
In FMC, navigate toDevices > Device Management.
Select the FTD device and configure route tracking to monitor the ISP links.
Configure SLA monitors to continuously check the health and performance of the internet circuits.
These configurations ensure that internet access remains available to users even if one of the ISPs goes down.
References:Cisco Secure Firewall Management Center Configuration Guide, Chapter on High Availability and SLA Monitoring.

質問: **5**
Cisco Secure Firewall Threat Defence デバイスは、インライン IPS モードに設定され、インライン セット内のインターフェイスを通過するすべてのトラフィックを検査します。VDB アップデートの適用中にトラフィックが中断されずに通過できるようにするには、インライン セット設定のどの項目を接続する必要がありますか？
A. リンク状態を伝播する
B. ショートフォールオープン
C. 厳格なTCP強制
D. タップモード
正解: **(**正解を表示します**)**

In inline IPS mode, to ensure that traffic passes through uninterrupted when VDB (Vulnerability Database) updates are being applied, the " Short Fall Open " setting must be configured. This setting allows traffic to continue to flow through the firewall even if there are issues with the inspection process, such as during updates or if the inspection engine fails.
Steps:
In FMC, navigate to the inline set configuration.
Enable the " Short Fall Open " option.
Deploy the configuration to the FTD device.
This ensures that network traffic is not disrupted during updates or other issues with the inspection process.
References:Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Inline IPS Mode Configuration.

質問**: 6**
エンジニアは、サードパーティのセキュリティ インテリジェンス テディを Cisco Secure Firewall Management Center に統合する必要があります。Secure Firewall Management Center はバージョン 6.2 3 で、メモリは 8 GB です。Throat Intelligence Director を実装するには、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. バージョン 6.6 にアップグレードします。
B. REST API アクセスを有効にします。
C. TAXII サーバーの URL を追加します。
D. 7 GB のメモリを追加します。
E. TAXII サーバーを追加します。
正解**: (**正解を表示します**)**
To integrate a third-party security intelligence feed with Cisco Secure Firewall Management Center (FMC) using Threat Intelligence Director (TID), the following actions are necessary:
Upgrade to version 6.6:The FMC must be running at least version 6.6 to support Threat Intelligence Director.
Version 6.2.3 does not support the necessary features for this integration.
Add the URL of the TAXII server:Threat Intelligence Director uses TAXII (Trusted Automated eXchange of Indicator Information) to pull threat intelligence data from third-party sources.
The URL of the TAXII server must be added to the TID configuration in FMC.
Steps:
Upgrade FMC to version 6.6 or later.
In FMC, navigate toIntegration > Threat Intelligence Director.
Add a new TAXII server by entering the URL of the TAXII server.
These actions enable the integration of third-party threat intelligence feeds, enhancing the security capabilities of the FMC.
References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Threat Intelligence Director.

質問**: 7**
ネットワーク管理者は、Cisco Secure Firewall Management Centerで管理されているCisco Secure Firewall Threat Defenseデバイスを、上流のBGPルータとルーティング情報を交換するように設定しています。管理者は、デバイスが上流ルータにアドバタイズしているネットワークを確認する必要があります。管理者はどのような操作を行う必要がありますか？
A. 詳細トラブルシューティングから show bgp neighbors NEIGHBOR-IP advertised-routes コマンドを実行します。
B. セキュアファイアウォール脅威防御デバイスのデバイスルーティング設定で 〝ルートインジェクション」を選択します。
C. Secure Firewall Management Center のデバイスルーティング設定で、[ルートインジェクション] を選択します。
D. Secure Firewall Management Center CLI から show route コマンドを実行します。
正解**: A (**コメントを発表する**)**

The show bgp neighbors NEIGHBOR-IP advertised-routes command displays the prefixes that the Secure Firewall Threat Defense device is advertising to a specific BGP neighbor. It must be executed against the managed threat defense device through the Advanced Troubleshooting interface. The ordinary show route command displays routes installed in the local routing table, not the specific prefixes advertised to a neighbor.
Route injection is a configuration capability and does not provide the required verification output. Cisco's command reference confirms that the advertised-routes keyword displays all routes advertised to the specified BGP peer, including the network, next hop, metric, weight, and AS path. Therefore, option A directly verifies the routes being shared with the upstream router. Cisco Secure Firewall Threat Defense Command Reference

質問: **8**
FTDユニットでどのコマンドを実行して、IPアドレス10.0.0.10にあり、登録キーCisco123を持つFMCマネージャーにユニットを関連付けますか？
A. ローカル10.0.0.10 Cisco123マネージャーの構成
B. configure manager add Cisco123 10.0.0.10
C. ローカルのCisco123 10.0.0.10マネージャーを構成する
D. configure manager add 10.0.0.10 Cisco123
正解: **(**正解を表示します**)**
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt- nw.html#id_106101

質問: **9**
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. 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
C. 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
D. 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
正解: **(**正解を表示します**)**

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. 別のウィジェットを追加します。
B. 別のタブを追加します。
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**
エンジニアは、Cisco FMC でリモート ストレージを設定する必要があります。構成のバックアップは、災害復旧のためにネットワーク上の安全な場所から入手できる必要があります。レポートは、監査人が Active Directory ログインでアクセスできる共有の場所にバックアップする必要があります。これらの目標を達成するために、エンジニアはどの戦略を使用する必要がありますか?
A. バックアップには SMB を使用し、レポートには NFS を使用します。
B. バックアップとレポートの両方に NFS を使用します。

C. バックアップとレポートの両方に SMB を使用します。
D. バックアップには SSH を使用し、レポートには NFS を使用します。
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
/system_configuration.html#ID-2241-00000551
"You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

質問: **12**
VPNユーザーは、接続を終了するCiscoFTDデバイスの背後にあるWebリソースを制限できません。
トラブルシューティング中に、ネットワーク管理者はDNS応答がCisco FTDを通過していないと判断しました。SnortIPSルールを使用しながら、この問題に対処するにはどうすればよいですか。
A. Snortルールを変更して、VPNユーザーへの正当なDNSトラフィックを許可します。
B. VPNフローの後にパケットを復号化して、DNSクエリが検査されないようにします
C. Snort処理を最適化するために、侵入ルールのしきい値を無効にします。
D. トラフィックを許可するには、侵入ポリシーの[インライン時にドロップ]チェックボックスをオフにします。
正解: (正解を表示します)

質問: **13**
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 Responseにイベントを直接送信することの利点は何ですか？
A. オンプレミスの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。
B. CiscoFirepowerデバイスをインターネットに接続する必要はありません。
C. すべてのタイプのCiscoFirepowerデバイスがサポートされています。
D. サポートされているバージョンのCiscoFirepowerを実行しているすべてのデバイスをサポートします。
正解: (正解を表示します)

質問: **14**
ある組織では、ブリッジグループを使用して内部インターフェースから外部インターフェースへのトラフィックを通過させるCisco FTDを使用しています。しかし、隣接するCiscoデバイスに関する情報を収集したり、環境内でマルチキャストを使用したりすることができません。この問題を解決するにはどうすればよいでしょうか？
A. 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。
B. 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。
C. ファイアウォール モードを透過に変更します。
D. ファイアウォール モードをルーティングに変更します。
正解: (正解を表示します)
" In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule... " " The bridge group does not pass CDP packets packets... "
https://www.cisco.com/c/en/us/td/docs/security/asa
/asa913/configuration/general/asa-913-general-config/intro-fw.html
Passing Traffic Not Allowed in Routed Mode
In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):

IP traffic-In routed firewall mode, broadcast and " multicast traffic is blocked even if you allow it in an access rule, " including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).
Non-IP traffic-AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.
Note
" The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

質問: **15**
ネットワーク管理者が、Cisco Secure Firewall Management Centerで特定のIPアドレスからの攻撃試行を確認しました。Secure Firewall Management CenterのWebインターフェイスから直接、そのIPアドレスに関する追加情報を取得するために使用できるCiscoセキュリティツールはどれですか？
A. Cisco Threat Response ブラウザプラグイン
B. シスコセキュアネットワークアナリティクス
C. Cisco Identity Services Engine
D. Cisco Secure Endpoint
正解: **A (**コメントを発表する**)**
The Cisco Threat Response browser plugin provides contextual investigation capabilities that can be launched from Secure Firewall Management Center. It allows an administrator to investigate an observable, such as a suspicious IP address, against Cisco threat-intelligence and integrated security sources without manually transferring the value to another interface. Secure Network Analytics analyzes network telemetry and behavior but is not the browser-based lookup mechanism described. Cisco ISE supplies identity, authorization, and network-access context, while Secure Endpoint provides endpoint telemetry and file or process investigation. Neither is the direct web-page investigation tool requested. Cisco documentation describes contextual cross-launch functionality for looking up suspicious source addresses in Cisco or third- party cloud-hosted intelligence services. Therefore, the Threat Response browser plugin is the correct selection. Cisco event investigation using web resources

質問: **16**
ネットワーク管理者が、Cisco Secure Firewall Management Centerに登録された透過型のCisco Secure Firewall Threat Defenseを設定しています。管理者は、ブリッジグループの2つのインターフェイス間でARPトラフィックが通過できるようにSecure Firewall Threat Defenseを設定したいと考えています。どのような設定が必要ですか？
A. アクセス ポリシーでは MAC アドレス FFFF.FFFF.FFFF を許可する必要があります。
B. デバイスのデフォルト設定を使用します。
C. アクセス ポリシーは MAC アドレス 0100.0CCC.CCCD を許可する必要があります。
D. ARP検査を無効にする必要があります。
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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

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. 利用できません

B不明
B. 切断された
C. きれい
正解: (正解を表示します)

質問: **18**
エンジニアは、Cisco FTD 上でパケットキャプチャを実行して、ホストが IP アドレスを使用していることを確認したいと考えている。
192 168.100.100 の MAC アドレスは 0042 7734.103 です。接続の問題のトラブルシューティングに役立ちます。パケット キャプチャ出力に MAC アドレスが表示されるようにするための正しい tcpdump コマンド構文は何ですか?
A. -nm src 192.168.100.100
B. -ソースなし 192.168.100.100
C. -w capture.pcap -s 1518 host 192.168.100.100 mac
D. -w capture.pcap -s 1518 host 192.168.100.100 ether
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**
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

質問: **20**
エンジニアがpxGridを使用してCisco FMCとCisco ISEを統合します。Cisco FMCにはどの役割が割り当てられますか？
A. 出版社
B. サーバー
C. クライアント
D. コントローラー
正解: (正解を表示します)

質問: **21**
同じサブネットのレイヤ 2 とレイヤ 3 でトラフィックを転送できるファイアウォール設計はどれですか?
A. Cisco Firepower Threat Defense モード
B. ルーテッド モード
C. ルーティングとブリッジングの統合
D. 透過モード
正解: (正解を表示します)

Transparent mode is a firewall configuration in which the firewall acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the firewall can forward traffic at both layer 2 and layer 3 for the same subnet, as it does not perform any address translation or routing. The firewall inspects the traffic and applies security policies based on the source and destination IP addresses, ports, and protocols. Transparent mode is useful when you want to deploy a firewall without changing the existing network topology or addressing scheme1.

質問: **22**
管理者は、ネットワークパフォーマンスを向上させるためにCisco FTDルールを最適化しており、Cisco FTDへの負荷を軽減するために特定のトラフィックタイプの検査をバイパスしたいと考えています。この目的を達成するには、どのポリシーを設定する必要がありますか？
A. プレフィルター
B. URLフィルタリング
C. 侵入
D. アイデンティティ
正解: **A (**コメントを発表する**)**

質問: **23**
エンジニアは、2 つの新しい Cisco FTD デバイスを構成して、既存のハイ アベイラビリティ ファイアウォール ペアを非常に安全な環境で置き換えています。フェールオーバー リンクを介して FTD デバイス間で交換される情報は、暗号化する必要があります。Cisco FTD でこれをサポートしているのはどのプロトコルですか?
A. IPsec
B. SSL
C. SSH
D. MACsec
正解: **(**正解を表示します**)**

質問: **24**

```
FMC: System > Monitor > [FTDv] > Advanced Troubleshooting > Capture w/Trace

1: 209.165.201.66.43410 > 209.165.202.100.8080: S 1349090467:1349090467(0) win
64240 <mss 1380,sackOK,timestamp 1421682252 0,nop,wscale 7>
 2: 209.165.202.100.8080 > 209.165.201.66.43410: R 0:0(0) ack 1349090468 win 0
 3: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425272499 0,nop,wscale 7>
 4: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
 admin prohibited filter
 5: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425273501 0,nop,wscale 7>
 6: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
 admin prohibited filter
 7: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425275517 0,nop,wscale 7>
 8: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
 admin prohibited filter
 9: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425279677 0,nop,wscale 7>
10: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
11: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
64240 <mss 1380,sackOK,timestamp 1425287869 0,nop,wscale 7>
12: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
13: 209.165.201.66.36438 > 209.165.202.143.8081: S 1804482258:1804482258(0) win
64240 <mss 1380,sackOK,timestamp 1425303997 0,nop,wscale 7>
14: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
15: 209.165.201.66.36438 > 209.165.202.143.8081: S 2230966104:2230966104(0) win
64240 <mss 1380,sackOK,timestamp 1425336509 0,nop,wscale 7>
16: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
```

図を参照してください。ユーザーは、さまざまなTCPポートを使用して多数の外部リソースに接続しようとします。ユーザーがポート番号を間違えると、接続は即座に切断され、接続が完全に切断されるまでに1分以上かかります。エンジニアは、図に示すように、両方のタイプの接続をキャプチャすることに成功しました。
エンジニアは、2番目の接続グループのタイムアウト値を下げてユーザーの問題を解決するために、どのような設定を行う必要があるでしょうか？
A. ICMPプロトコルスイート全体を許可する送信アクセスルール
B. 外部からのTCPリセットパケットを許可する受信アクセスルール
C. リセットアクション付きブロックの送信アクセスルール
正解: (正解を表示します)

質問: **25**
ネットワーク管理者は、Cisco Secure Firepower Management Center を使用して、データセンター内の複数のファイアウォールを含むネットワークを管理しています。管理者は、次世代ファイアウォールをルーテッドモードからトランスペアレントモードに変更する必要があります。この要件を満たすために、管理者は次にどのようなアクションを実行する必要がありますか？
A. CLI からインターフェイス設定を手動で削除します。
B. CLI から configure transparent firewall コマンドを入力します。
C. CLI から 1 つ以上のブリッジ グループを作成します。
D. Cisco Secure Firewall Management Center でファイアウォールの登録を解除します。
正解: (正解を表示します)

質問: **26**
ネットワーク管理者は、Cisco Secure Firewall Management Center に登録されている Cisco Secure Firewall Threat Defence インスタンスへの VPN 認証用に Active Directory 認証を設定しようとしています。この目標を達成するには、まず Secure Firewall Management Center でどのシステム設定を設定する必要がありますか?

A. デバイス、リモート アクセス VPN
B. システム、レルム
C. ポリシー、認証
D. 認証、デバイス
正解: **B (**コメントを発表する**)**
To configure Active Directory authentication for VPN authentication on a Cisco Secure Firewall Threat Defense (FTD) instance registered with Cisco Secure Firewall Management Center (FMC), the administrator needs to configure Realms in the System settings of the FMC. Realms in FMC are used to define the directory servers (e.g., Active Directory) and how they are used for user authentication.
Steps to configure this in FMC:
Navigate toSystem > Integration > Realms and Directory.
Add a new realm and configure the necessary details such as the directory server type (e.g., Active Directory), server address, and bind credentials.
Test the connection to ensure it works correctly.
This setup allows the FMC to authenticate VPN users against the Active Directory, thereby enabling secure access control for VPN connections.
References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Realms Configuration.

質問: **27**
エンジニアが、Cisco Secure Firewall Management Centerで管理されているCisco Secure Firewall Threat Defenceデバイスを設定しています。このデバイスでは、リモート管理のためにSSHが有効になっており、内部インターフェイスからアクセス可能である必要があります。エンジニアは、これを実現するためにどのタイプのポリシーを設定する必要がありますか？
A. 識別する
B. アクセス制御
C. プレフィルター
D. プラットフォーム設定
正解: **(**正解を表示します**)**
To enable SSH access to a Cisco Secure Firewall Threat Defense (FTD) device from the inside interface for remote administration, the engineer needs to configure a Platform Settings policy in Cisco Secure Firewall Management Center (FMC). The Platform Settings policy allows the configuration of various system-related settings, including enabling SSH, specifying the allowed interfaces, and defining the SSH access parameters.
Steps:
In FMC, navigate toPolicies > Access Control > Platform Settings.
Create a new Platform Settings policy or edit an existing one.
In the policy settings, go to theSSHsection.
Enable SSH and specify theinsideinterface as the allowed interface for SSH access.
Define the SSH parameters such as allowed IP addresses, user credentials, and other security settings.
Save and deploy the policy to the FTD device.
This configuration ensures that SSH access is enabled on the specified interface, allowing secure remote administration.
References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings.

質問: **28**
セキュリティエンジニアが、リソースとインターネット帯域幅が制限されているリモートCiscoFTDを設定しています。クラウドルックアップの要件を減らすために、どのマルウェアアクションと保護オプションを構成する必要がありますか？

A. ブロックファイルアクションとローカルマルウェア分析
B. マルウェアアクションとローカルマルウェア分析をブロックする
C. マルウェアクラウドルックアップと動的分析
D. マルウェアのアクションと動的分析をブロックする
正解: **B** (コメントを発表する)

質問: **29**



図を参照してください。エンジニアが、以下のハードウェアデバイスとソフトウェアバージョンを備えた高可用性ソリューションを構成しています。
FXOS SW 2.0(1.23) ソフトウェアを搭載した Cisco Secure Firewall 9300 セキュリティ アプライアンス 2 台、両方のアプライアンスに Cisco Secure Firewall Threat Defense 6.0.1.1 (ビルド 1023) がインストールされています。また、SW 6.0.1.1 (ビルド 1023) を搭載した Cisco Secure Firewall Management Center が 1 台あります。高可用性構成を完了するには、どの条件を満たす必要がありますか？
A. バージョン番号は同じパッチ番号である必要があります。
B. DHCPは少なくとも1つのファイアウォールインターフェースで設定する必要があります。
C. 両方のファイアウォールは透過モードである必要があります。
D. 両方のファイアウォールは同じ数のインターフェースを持つ必要があります。
正解: (正解を表示します)

質問: **30**
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: **B** (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/reusable_objects.html

質問: **31**
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 "show tech" file for the device in question
B. A "show tech" for the Cisco FMC.
C. A "troubleshoot" file for the Cisco FMC
D. A Troubleshoot" file for the device in question.
正解: **D (**コメントを発表する**)**

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 **446**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
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。
D. 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。
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**)**
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699- configure-ftd-high-availability-on-firep.html

質問: **33**
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. 間違ったIPアドレスが使用されています。
C. 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。
D. ディレクトリの場所が正しくありません。
正解: **(**正解を表示します**)**
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

質問: **34**
エンジニアは、CiscoFTDセンサーの設定をプルしてCiscoTACで確認しようとしますが、デバイスのCUに直接アクセスすることはできません。デバイスのCL1は、エンジニアがアクセスできるCiscoFMCによって管理されます。Cisco FMCのどのアクションが、デバイスのCL1へのアクセスを許可しますか。
A. CiscoFMCの[FileDownload]セクションで設定ファイルをダウンロードします。

B. CiscoFMC内に設定のバックアップを作成します。
C. CiscoFMC内のインポート/エクスポートツールを使用して設定をエクスポートします。
D. CiscoFMC内のCiscoFTDCLI機能でshowrunallコマンドを使用します。
正解: **(**正解を表示します**)**

質問: **35**
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。これの原因は何ですか？
A. 非管理インターフェースに割り当てられた最大MTUの値が変更されました。
B. 非管理インターフェー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. 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。
正解: **(**正解を表示します**)**

質問: **36**
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: **37**
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. コアダンプパケットエンジンを有効にする
B. キャプチャトラフィック
C. キャプチャ
D. WORDをキャプチャする
正解: **C (**コメントを発表する**)**
Reason: the command " capture-traffic " is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the " capture " command. Since the Lina Engine represents the actual physical interface of the device, " capture " is the only reasonable choice Reference:https://www.cisco.com/c/en/us/support/docs /security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10 The command is firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

質問: **38**
エンジニアは、Cisco Secure Firewall Management Centerを使用して、Cisco Secure IPS上でERSPANパッシブインターフェイスを設定する必要があります。以下の設定は既に完了しています。
パッシブインターフェースを設定します。

ERSPANのIPアドレスを設定してください。
設定を完了するために、追加で設定する必要がある項目はどれですか？(2つ選択してください。)
A. フローID
B. バイパスモード
C. 送信元IPアドレス
D. TCPインターセプト
E. 宛先MAC
正解: **(**正解を表示します**)**

質問: **39**
ネットワーク管理者は、CiscoFTDでのVPNユーザ認証のためにLDAPからLDAPSに変換しようとしています。このタスクを実行するには、Cisco FTDオブジェクトに対してどのアクションを実行する必要がありますか？
A. LDAPS暗号スイートを識別し、暗号スイートリストオブジェクトを使用してCiscoFTD接続要件を定義します。
B. 必要なLDAPS証明書を取得するための証明書登録オブジェクトを作成します。
C. LDAPS証明書を取得するためのキーチェーンオブジェクトを追加します。
D. ポリシーリストオブジェクトを変更して、LDAPSのセッション要件を定義します。
正解: **(**正解を表示します**)**

質問: **40**
エンジニアは、Secure Firewall Threat Defense デバイスの問題のトラブルシューティングを支援するために、Cisco Secure Firewall Management Center 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。エンジニアが Secure Firewall Management Center の URL にアクセスすると、次のようになります。
.. < FMC IP > /capture/CAP/pcap/sample.pcap
エンジニアは、PCAPファイルを受け取る代わりに、403: Forbiddenエラーを受け取りました。この問題を解決するには、どのような対処法が有効でしょうか？
A. HTTPSサーバーを無効にしてHTTPを使用します。
B. デバイスプラットフォームポリシーでプロキシ設定を有効にします。
C. デバイスプラットフォームポリシーでHTTPSを有効にします。
D. クライアント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**)**
If an engineer receives a 403: Forbidden error when attempting to download a packet capture file from Cisco Secure Firewall Management Center (FMC), the issue is likely due to HTTPS not being enabled in the device platform policy. To resolve this issue, the engineer must enable HTTPS in the platform policy.
Steps:
In FMC, navigate toPolicies > Device Management > Platform Settings.
Edit the relevant platform policy.
Enable HTTPS for the device.
Deploy the changes to the FTD device.
This ensures that the FMC and FTD device can securely transfer the packet capture file over HTTPS, resolving the 403 error.
References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings and HTTPS Configuration.

質問: **41**
エンジニアは、現在の6.2.3展開にCisco FTDバージョン6.2.3デバイスを追加して、ハイアベイラビリティペアを作成したいと考えています。

現在展開されているCiscoFTDデバイスは、ローカル管理と、使用可能なポート密度を含む同一のハードウェアを使用して、適切なハイアベイラビリティ展開に必要なフェールオーバーとステートフルリンクを有効にします。環境が新しいCiscoFTDを古いものとペアリングする準備ができていることを確認するアクションはどれですか。
A. 名前解決のために、構成されたDNSサーバーが2つのデバイスで一致していることを確認します。
B. 両方のデバイスでCiscoFDM管理からCiscoFMC管理に変更し、FMCに登録します。
C. フェールオーバーインターフェイス用に、2つのデバイスに169 254.0.0/16の範囲のIPアドレスが割り当てられていることを確認します。
D. 現在のCisco FTDを工場出荷時の状態にリセットして、設定を新しいCiscoFTDデバイスと同期できるようにします。
正解: **(**正解を表示します**)**

質問: **42**
エンジニアは、CiscoFirepower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 cluster interface mode
B. in active/active mode
C. in active/passive mode
D. in a cluster span EtherChannel
正解: **(**正解を表示します**)**

質問: **43**
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. システムは ssl-client-hello-force-reset をサポートします
B. システムはssl-client-hello-tuningをサポートします
C. システムがssl-client-hello-enabledをサポート
D. システムはssl-client-hello-displayをサポートします
正解: **(**正解を表示します**)**

質問: **44**
インラインセットプロパティの下の詳細タブで、インターフェイスがパッシブインターフェイスをエミュレートできるようにしますか？
A. 透過インラインモード
B. TAPモード
C. 厳密なTCP強制
D. リンク状態を伝達する
正解: **(**正解を表示します**)**
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

質問: **45**
Cisco Threat Response によるインシデント調査を簡素化するコンポーネントはどれですか?
A. Cisco AMP クライアント
B. ローカル CVE データベース
C. Cisco Secure Firewall アプライアンス

D. ブラウザプラグイン
正解: (正解を表示します)
Cisco Threat Response (CTR) is a security solution that helps simplify incident investigation and threat hunting. One of its components that significantly simplifies the investigation process is the browser plug-in.
The browser plug-in integrates with CTR to provide contextual information directly within the browser, allowing security analysts to quickly view threat details, pivot to related information, and take appropriate actions without switching between multiple tools.
Features of the browser plug-in:
* Provides real-time threat intelligence and context from various Cisco security products.
* Allows security analysts to investigate incidents directly from web-based consoles.
* Enhances efficiency by streamlining the workflow and reducing the time needed to gather and correlate information.
References:Cisco Threat Response Documentation, Browser Plug-in Section.

質問: **46**
Cisco ISEをCisco FMCと統合して脅威を迅速に封じ込めるために使用されるコネクタはどれですか。
A. pxGrid
B. FMC RTC
C. ISEGrid
D. FTD RTC
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 **446**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

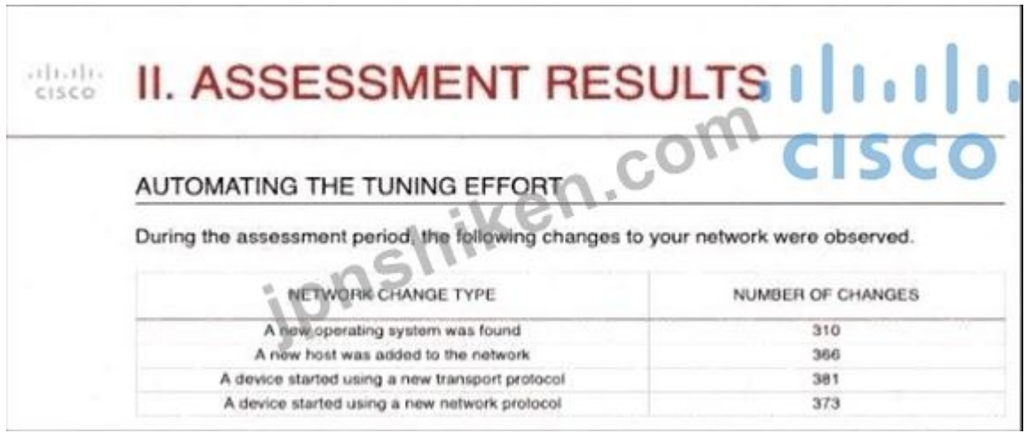
質問: **47**


図を参照してください。エンジニアが、インターフェースをIPSインラインペアモードにしてCisco Secure Firewall Threat Defenseのインスタンスを設定しています。要件を満たすために、インターフェースe1/6には何を設定する必要がありますか？
A. リンク状態の伝播が無効になっています
B. セキュリティゾーンをOUTSIDE_ZONEに設定
C. インラインセットMTUを1500に設定

D. フェイルセーフ無効
正解: (正解を表示します)

質問: **48**
pxGrid Adaptive Network ControlをCisco ISEおよびCisco Secure Firewall Management Centerと統合することで、Cisco Rapid Threat Containmentのどの緩和策が有効になりますか？
A. 終了
B. ブロック
C. 拒否
D. 一時停止
正解: (正解を表示します)

質問: **49**
図を参照してください。



エンジニアが攻撃リスクレポートを分析したところ、ネットワーク上で 300 を超える新しいオペレーティングシステムが見つかりました。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. Cisco Firepower はポリシーを自動的に更新します。
B. 管理者は Cisco Firepower から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. 管理者はポリシーを手動で更新します。
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: **50**
CiscoFTDデバイスのIRBでサポートされている機能はどれですか。
A. 動的ルーティングプロトコル
B. 高可用性クラスター
C. EtherChannelインターフェース
D. 冗長インターフェース
正解: **A** (コメントを発表する)

質問: **51**
Cisco Rapid Threat Containment がネットワーク内の脅威を封じ込めるために使用する方法は何ですか?
A. 認証の変更
B. コンテキストデータの共有
C. トラストセグメンテーション
D. TACACS+
正解: **(**正解を表示します**)**

質問: **52**
Cisco FMCを介してデバイスを管理しながらデバイスを削除および再追加する場合、どの2つの考慮事項を考慮する必要がありますか (2つ選択してください)。
A. デバイスが削除されたら、CiscoFMCに再追加する前に再設定する必要があります。
B. 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ありません。そのため、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。
C. 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可能であるため、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。
D. デバイスを再度追加する前にCisco FMCでは、マネージャを再度追加する必要があります。
E. 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に要求します。
正解: **(**正解を表示します**)**

質問: **53**
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. 攻撃リスクレポート
B. ネットワークリスクレポート
C. ユーザーリスクレポート
D. 高度なマルウェアリスクレポート
正解: **(**正解を表示します**)**

質問: **54**
Cisco Firepower Threat Defense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受動的に受信するように構成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. インラインセット
B. パッシブ
C. ルーティング済み
D. インラインタップ
正解: **(**正解を表示します**)**
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/interface_overview_for_firepower_threat_defense.html

質問: **55**
どのファイアウォール設計であれば、同じサブネットに対してレイヤー2とレイヤー3の両方でトラフィックを転送できますか？
A. 透明モード
B. ルーティングモード

C. 統合ルーティングおよびブリッジング
D. Cisco Firepower Threat Defenseモード
正解: **A** (コメントを発表する)

質問: **56**
ネットワーク管理者は、パブリックIPアドレスを内部WebサーバーのIPアドレスに変換するNATポリシーを構成しました。どのソースもポート80のパブリックIPアドレスに到達できるようにするアクセスポリシーも作成されています。インターネットからポート80でWebサーバーにアクセスすることはできません。どの構成変更が必要ですか。
A. アクセスポリシーは、内部WebサーバーのIPアドレスへのトラフィックを許可する必要があります。
B. 送信元IPアドレスと宛先IPアドレスを変換するには、NATポリシーを変更する必要があります。
C. ポート80では侵入ポリシーを無効にする必要があります。
D. アクセスポリシールールは、アクションの信頼のために構成する必要があります。
正解: **A** (コメントを発表する)

質問: **57**
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. 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。
B. 悪意のあるファイルをブロックリストに追加します。
C. 調査結果を外部の脅威分析エンジンに転送する。
D. 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。
正解: **B** (コメントを発表する)

質問: **58**
ある組織は、IPS機能のないCisco Firepowerを導入しましたが、トラフィックの検査を有効にしたいと考えています。プロトコルの異常を検出し、Snortルールセットを使用して悪意のある動作を検出できるようにする必要があります。これはどのように実現できますか？
A. アクセス制御ポリシーを変更して、興味深いトラフィックをエンジンにリダイレクトします。
B. 検査対象となる新しいホストを検出するために、ネットワーク検出ポリシーを変更します。
C. 侵入ポリシーを変更して、検査対象となるイベントの最小深刻度を決定します。
D. ネットワーク分析ポリシーを変更して、検査対象のパケットを処理する
正解: (正解を表示します)

質問: **59**
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: **B,C** (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/reusable_objects.html#ID-2243-00000414

質問: **60**
ある会社は、Cisco FMC によって管理される複数の Cisco FTD アプライアンスに侵入保護を展開しています。速度と検出が優先される場合、どのシステム提供ポリシーを選択する必要がありますか?
A. バランスの取れたセキュリティと接続性
B. 接続上のセキュリティ
C. 最大検出
D. セキュリティよりも接続性
正解: **(**正解を表示します**)**

質問: **61**
Cisco FMC GUIを介したCisco NGFWの初期導入時に、ローカルDMZの導入に含まれるポリシールールはどれですか。
A. ip anyを拒否する
B. ポリシールールが含まれていない
C. 許可ip任意
D. ユーザーのみがIPアドレスを変更できるデフォルトのDMZポリシー。
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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
ネットワーク管理者は、Cisco Secure Firewall Management Center で過去 24 時間に行われた変更を説明する日次電子メール レポートを管理者に送信する必要があります。どのシステム設定を有効にする必要がありますか?
A. STIG準拠
B. 監査ログをSyslogに送信
C. 変更調整
D. 監査ログをHTTPサーバーに送信
正解: **C (**コメントを発表する**)**
Change Reconciliation is specifically designed to generate and email a detailed summary of configuration changes made during the preceding 24 hours. Secure Firewall Management Center takes snapshots when users save configuration changes and consolidates those records into a daily change report. The administrator can enable the feature, select the scheduled delivery time, specify recipient email addresses, and optionally include the full change history. Sending audit logs to a syslog or HTTP server exports individual audit events to an external system but does not automatically generate the required daily management report. STIG Compliance evaluates the system against security configuration guidance and is unrelated to change reporting.
Therefore, Change Reconciliation is the only option that directly satisfies both the 24-hour reporting period and email-delivery requirements. Cisco Change Reconciliation configuration

質問: **63**

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. box lever chart
B. arrow chart
C. bar chart
D. benchmark chart
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: **64**
Cisco Secure Firewall デバイスで IRB モードの分離されたブリッジ グループを設定するには、どのアクションを実行する必要がありますか?
A. 制限されたセグメントを ACL に追加します。
B. BVI インターフェイス名は空のままにします。
C. ブロックされたトラフィックの NAT プールを定義します。
D. ルーティング テーブルからルートを削除します。
正解: **B (**コメントを発表する**)**
To configure an isolated bridge group for Integrated Routing and Bridging (IRB) mode on a Cisco Secure Firewall device, the action to take is to leave the BVI (Bridge Virtual Interface) interface name empty. This ensures that the bridge group operates in an isolated manner, where Layer 3 routing is not applied to the bridged interfaces, effectively isolating the traffic within the bridge group.
Steps:
* Access the firewall's configuration interface.
* Configure the bridge group interfaces.
* Ensure that the BVI interface name is left empty to isolate the bridge group.
This configuration prevents Layer 3 routing for the isolated bridge group, ensuring that traffic remains contained within the bridge group.
References:Cisco Secure Firewall Management Center Configuration Guide, Chapter on Bridge Groups and IRB Mode.

質問: **65**
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. 単一展開
C. シングルコンテキスト
D. マルチインスタンス
正解: **(**正解を表示します**)**

質問: **66**
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: **67**
管理者は、Cisco Secure Firewall Management Center 内の保存された検索から新しいレポート テンプレートを設定しています。目標は、マルウェア分析レポート テンプレートを使用することですが、ベースとして異なるタイプの保存された検索を使用します。レポートが機能しません。このレポート テンプレートを設定する際に考慮すべきことは何ですか?
A. 保存した検索は同じレポートテンプレートにのみ使用できます
B. 保存された検索は、同じドメイン内のすべてのレポート テンプレートで自由に使用できます。
C. 別のレポート テンプレートから保存された検索を使用する必要があります。
D. 保存した検索は、別のレポート テンプレートに使用する前に名前を変更する必要があります。
正解: (正解を表示します)
When configuring a new report template based on a saved search in Cisco Secure Firewall Management Center (FMC), it is important to note that saved searches are specific to the report template they were created with. Saved searches cannot be freely used across different report templates.
To use a different type of saved search, you must ensure that it aligns with the specific report template being used. This restriction ensures that the saved search parameters match the report's data requirements.
References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Reporting and Saved Searches.

質問: **68**
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. 特権
B. ユーザー
C. 構成
D. 管理者
正解: (正解を表示します)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config- guide-v66/command_line_reference.pdf

質問: **69**

```
Network_1;Internal network;192.168.1.0/24;
FQDN_1;Domain Names;FQDN;www.example.com;ipv4_ipv6
Network_2;Internal network2;192.168.2.0/24;
```

図を参照してください。エンジニアは、CSVファイルを使用して3つのネットワークオブジェクトをCisco Secure Firewall Management Centerにインポートする必要があります。このタスクを実行するには、CSVファイルでどのヘッダーを設定する必要がありますか？
A. 名前;説明; タイプ;値;DN;
B. 名前; 説明; タイプ; 値; ルックアップ;
C. 名前;説明;タイプ;値;検索;
D. 名前; 説明; タイプ; 値; DN;
正解: **C** (コメントを発表する)

質問: **70**

CiscoUmbrellaをCiscoThreat Responseと統合している間、ネットワークセキュリティエンジニアは、ドメインのブロッキングをCisco ThreatResponseインターフェイスからCiscoUmbrellaに自動的にプッシュしたいと考えています。どのAPIがこの要件を満たしていますか？

A. REST

B. レポート

C. 調査する

D. 強制

正解: **(**正解を表示します**)**

質問: **71**

```
ASA# show interface | include ",|MAC|Member
Interface GigabitEthernet1/1 "inside", is up, line protocol is up
        MAC address e4aa.5ae4.612e, MTU 1500
Interface GigabitEthernet1/2 "outside", is up, line protocol is up
        MAC address e4aa.5ae4.612f, MTU 1500
Interface GigabitEthernet1/3 "", is up, line protocol is up
        MAC address 500f.8000.bbb5, MTU 1500
Interface GigabitEthernet1/4 "", is up, line protocol is up
        MAC address 500f.8000.bbb6, MTU 1500
Interface GigabitEthernet1/5 "", is up, line protocol is up
        MAC address 500f.8000.bbb7, MTU 1500
Interface GigabitEthernet1/6 "", is up, line protocol is up
        MAC address 500f.8000.bbb8, MTU 1500
Interface GigabitEthernet1/7 "", is up, line protocol is up
        MAC address 500f.8000.bbb9, MTU 1500
Interface GigabitEthernet1/8 "", is up, line protocol is up
        MAC address 500f.8000.bbba, MTU 1500
Interface Management1/1 "", is up, line protocol is up
        MAC address 500f.8000.bbb2, MTU 1500
Interface Redundant1 "Redundant1", is up, line protocol is up
        MAC address 500f.8000.bbb3, MTU 1500
        Member GigabitEthernet1/3(Active), GigabitEthernet1/4
```

図を参照してください。エンジニアは、Cisco ASAファイアウォールとCisco Secure Firewall Services Moduleとの接続を設定し、プライマリインターフェイスに障害が発生した場合にセカンダリインターフェイスがプライマリインターフェイスのすべての機能を引き継ぐようにする必要があります。下部にあるコードスニペットをCLIコマンドのボックスにドラッグアンドドロップして、フェイルオーバーを設定してください。すべてのオプションを使用するわけではありません。

```
ASA(config)#interface
ASA(config-if)#
ASA(config-if)#
ASA(config-if)# nameif Redundant1
ASA(config-if)# security-level 20
ASA(config-if)# ip address 172.16.47.1
ASA(config-if)# end

ASA# show version | include Gigabit.*address is
 1: Ext: GigabitEthernet1/1  : address is 500f.8000.bbb3, irq 255
 2: Ext: GigabitEthernet1/2  : address is 500f.8000.bbb4, irq 255
 3: Ext: GigabitEthernet1/3  : address is 500f.8000.bbb5, irq 255
 4: Ext: GigabitEthernet1/4  : address is 500f.8000.bbb6, irq 255
 5: Ext: GigabitEthernet1/5  : address is 500f.8000.bbb7, irq 255
 6: Ext: GigabitEthernet1/6  : address is 500f.8000.bbb8, irq 255
 7: Ext: GigabitEthernet1/7  : address is 500f.8000.bbb9, irq 255
 8: Ext: GigabitEthernet1/8  : address is 500f.8000.bbba, irq 255
```

member-interface GigabitEthernet1/5	member-interface GigabitEthernet1/4
GigabitEthernet1/5	backup interface GigabitEthernet1/4
Redundant1	reactivation mode timed
failover link Redundant1 GigabitEthernet1/4	

正解:

jpnshiken.com

```
ASA(config)#interface Redundant1
ASA(config-if)# GigabitEthernet1/5
ASA(config-if)# member-interface GigabitEthernet1/4
ASA(config-if)# nameif Redundant1
ASA(config-if)# security-level 20
ASA(config-if)# ip address 172.16.47.1
ASA(config-if)# end

ASA# show version | include Gigabit.*address is
  1: Ext: GigabitEthernet1/1  : address is 500f.8000.bbb3, irq 255
  2: Ext: GigabitEthernet1/2  : address is 500f.8000.bbb4, irq 255
  3: Ext: GigabitEthernet1/3  : address is 500f.8000.bbb5, irq 255
  4: Ext: GigabitEthernet1/4  : address is 500f.8000.bbb6, irq 255
  5: Ext: GigabitEthernet1/5  : address is 500f.8000.bbb7, irq 255
  6: Ext: GigabitEthernet1/6  : address is 500f.8000.bbb8, irq 255
  7: Ext: GigabitEthernet1/7  : address is 500f.8000.bbb9, irq 255
  8: Ext: GigabitEthernet1/8  : address is 500f.8000.bbba, irq 255
```

member-interface GigabitEthernet1/5

member-interface GigabitEthernet1/4

GigabitEthernet1/5

backup interface GigabitEthernet1/4

Redundant1

reactivation mode timed

failover link Redundant1 GigabitEthernet1/4

jpnshiken.com

Explanation:

A screenshot of a computer AI-generated content may be incorrect.



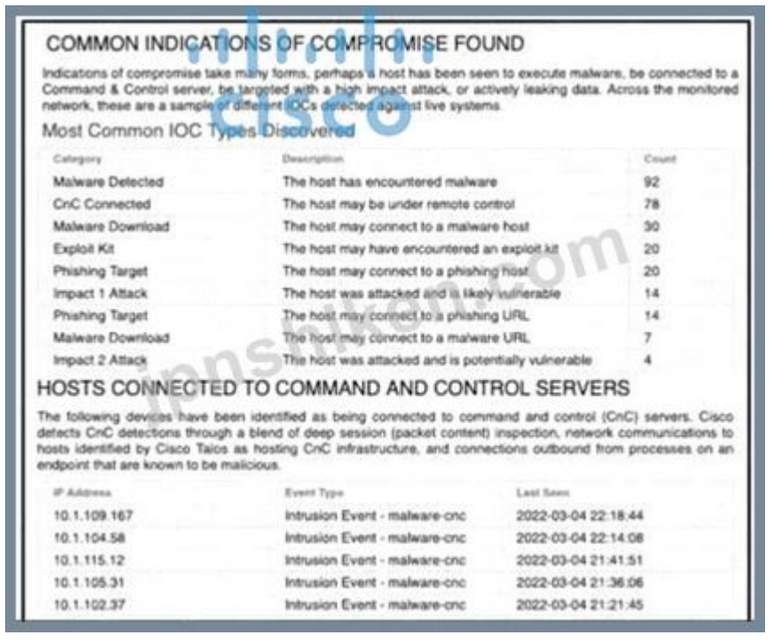
質問: **72**
エンジニアが、Cisco Secure Firewall 上の既存のカスタムサーバーフィンガープリントを見直しています。現在の情報が不正確であるためです。ネットワーク検出ルールの精度を向上させるために、エンジニアはどのような措置を講じる必要がありますか？
A. スキップする必要のあるポートを除外します。
B. ネットワークセグメントのNetFlow監視を追加します。
C. マルチドメイン環境でレポートを上書きするための共通ルールを1つ設定します。
D. 監視対象ホストとの通信に使用されるIPアドレスを除外します。
正解: **(**正解を表示します**)**

質問: **73**
エンジニアは Cisco FTD デバイスを導入する必要があります。管理者は、エンド ユーザーに混乱をもたらすネットワーク変更を必要とせずにトラフィックを調査したいと考えています。企業のセキュリティ ポリシーでは、管理トラフィックをデータ トラフィックから分離し、リモート管理に Telnet 経由の SSH を使用することが必要です。これらの要件を満たすには、デバイスをどのように展開する必要がありますか?
A. 診断インターフェイスを使用したルーテッド モード
B. 管理インターフェイスを使用した透過モード
C. データインターフェイスで作成された透明な
D. ブリッジ仮想インターフェイスを使用したルーテッド モード
正解: **(**正解を表示します**)**
To deploy a Cisco FTD device that meets the requirements of the question, the engineer must use transparent mode with a management interface. Transparent mode is a firewall configuration in which the FTD device acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the FTD device can examine traffic without requiring network changes that will disrupt end users, such as changing IP addresses or routingconfigurations1. A management interface is a dedicated interface that is used for managing the FTD device and separating management traffic from data traffic. A management interface can be configured to allow SSH access for remote administration, which is more secure than Telnet2.
The other options are incorrect because:
* Routed mode is a firewall configuration in which the FTD device acts as a router and performs address translation and routing for connected networks. Routed mode requires network changes that may disrupt end users, such as changing IP addresses or routing configurations1. A diagnostic interface is a special interface that is used for troubleshooting and capturing traffic on the FTD device. A diagnostic interface does not separate management traffic from data traffic or allow SSH access for remote administration.

* Transparent mode with a data interface does not meet the requirement of separating management traffic from data traffic. A data interface is a regular interface that is used for passing and inspecting traffic on the FTD device. A data interface does not allow SSH access for remote administration2.
* Routed mode with a bridge virtual interface (BVI) does not meet the requirement of examining traffic without requiring network changes that will disrupt end users. A BVI is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. A BVI allows the FTD device to route between different bridge groups on the same security module/engine. However, routed mode still requires network changes that may disrupt end users, such as changing IP addresses or routing configurations.

質問: **74**
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. configure manager add <FMC IP> ACME0O1 <登録キー>
B. configure manager add ACME001 <registration key> <FMC IP>
C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <登録キー>
D. マネージャーの追加<FMCIP>登録キー> ACME001を構成します
正解: **D** (コメントを発表する)

質問: **75**


COMMON INDICATIONS OF COMPROMISE FOUND

Indications of compromise take many forms, perhaps a host has been seen to execute malware, be connected to a Command & Control server, be targeted with a high impact attack, or actively leaking data. Across the monitored network, these are a sample of different IOCs detected against live systems.

Most Common IOC Types Discovered

Category	Description	Count
Malware Detected	The host has encountered malware	92
CnC Connected	The host may be under remote control	78
Malware Download	The host may connect to a malware host	30
Exploit Kit	The host may have encountered an exploit kit	20
Phishing Target	The host may connect to a phishing host	20
Impact 1 Attack	The host was attacked and is likely vulnerable	14
Phishing Target	The host may connect to a phishing URL	14
Malware Download	The host may connect to a malware URL	7
Impact 2 Attack	The host was attacked and is potentially vulnerable	4

HOSTS CONNECTED TO COMMAND AND CONTROL SERVERS

The following devices have been identified as being connected to command and control (CnC) servers. Cisco detects CnC detections through a blend of deep session (packet content) inspection, network communications to hosts identified by Cisco Talos as hosting CnC infrastructure, and connections outbound from processes on an endpoint that are known to be malicious.

IP Address	Event Type	Last Seen
10.1.109.167	Intrusion Event - malware-cnc	2022-03-04 22:18:44
10.1.104.58	Intrusion Event - malware-cnc	2022-03-04 22:14:08
10.1.115.12	Intrusion Event - malware-cnc	2022-03-04 21:41:51
10.1.105.31	Intrusion Event - malware-cnc	2022-03-04 21:36:06
10.1.102.37	Intrusion Event - malware-cnc	2022-03-04 21:21:45

図を参照してください。エンジニアがCisco Secure Firewall Management Centerのネットワークリスクレポートを分析しています。このリスクを軽減するために、エンジニアはどのような対策を推奨すべきでしょうか？
A. トレンド分析
B. ネットワークベースの検出
C. 仮想保護
D. IPアドレスとURLのブラックリスト登録
正解: (正解を表示します)

質問: **76**

組織は、新しい Cisco Firepower ハイ アベイラビリティ展開を構成しています。フェールオーバーがエンド ユーザーにとって可能な限りシームレスであることを保証するには、どのアクションを実行する必要がありますか?
A. シャーシ間の仮想フェイルオーバー MAC アドレスを設定します。
B. 両方のシャーシに同じソフトウェア バージョンをロードします。
C. シャーシ間に専用のステートフル リンクを使用します。
D. 両方のシャーシに同じ FQDN を設定します。
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
446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-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

質問: **78**
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: (正解を表示します)
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: **79**
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が適用される前に有効化されていませんでした
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: **80**
最近追加された新しいサーバーが、現在ファイアウォールで分離されている既存のサーバーと通信する必要があるため、エンジニアはCisco Secure Firewallの透過モードを実装する必要があります。この目的を達成するために、エンジニアは次にどのような実装アクションを実行する必要がありますか？
A. 両方のサーバーに同じデフォルトゲートウェイを設定します。
B. 両方のサーバーが同じVXLANセグメントを共有できるようにします。
C. 両方のサーバーに同じサブネットを割り当てます。
D. 両方のサーバーが同じブリッジドメインに属していることを確認してください。
正解: **D (**コメントを発表する**)**

質問: **81**
エンジニアが Cisco FMC でカスタム侵入ルールを設定しています。エンジニアは、ペイロードまたはストリームから文字列 " |45 5* 26 27 4 0A|* を検索するルールが必要です。パックされた検査の引数を作成するために、エンジニアはこの文字列とともにどのキーワードを使用する必要がありますか?
A. メタデータ
B. 内容
C. 保護されたコンテンツ
D. データ
正解: **(**正解を表示します**)**
The content keyword is used to specify a string or pattern to search for in the payload or stream of a packet.
The string must be enclosed in quotation marks and can use modifiers such as nocase, depth, offset, and so on.
The string can also use hexadecimal notation by using a pipe symbol (|) before and after the hexadecimal characters. For example, content: " |45 5* 26 27 4 0A| " will match any payload or stream that contains the hexadecimal bytes 45 5 26 27 4 0A followed by any number of bytes2

質問: **82**
管理者は、パッシブIPS展開環境において、Cisco Secure Firewall Threat Defenseデバイスのインターフェイスを設定しています。デバイスとインターフェイスは既に識別されています。実装を完了するために、管理者は次にどの設定手順を実行すればよいでしょうか？
A. インターフェースモードをパッシブに設定します。インターフェースをセキュリティゾーンに関連付けます。MTUパラメータを設定します。
インターフェースをリセットします。
B. 受信したトラフィックを再送信するようにインターフェースを変更します。インターフェースをセキュリティゾーンに関連付けます。インターフェースを有効にします。MTU パラメータを設定します。
C. 受信したトラフィックを再送信するようにインターフェースを変更します。インターフェースをセキュリティゾーンに関連付けます。MTUパラメータを設定します。
D. インターフェースモードをパッシブに設定します。インターフェースをセキュリティゾーンに関連付けます。インターフェースを有効にします。MTUパラメータを設定します。
正解: **(**正解を表示します**)**
In a passive IPS deployment for a Cisco Secure Firewall Threat Defense (FTD) device, the administrator must configure the interface to operate in passive mode. This involves setting the interface mode, associating it with a security zone, enabling the interface, and setting the MTU parameter.
Steps:
Set the interface mode to passive:
In FMC, navigate toDevices > Device Management.

Select the FTD device and configure the relevant interface.
Set the interface mode to " Passive. "
Associate the interface with a security zone:
Create or select an appropriate security zone.
Assign the passive interface to this security zone.
Enable the interface:
Ensure the interface is enabled to receive traffic.
Set the MTU parameter:
Configure the Maximum Transmission Unit (MTU) parameter as required.
This ensures that the FTD device can inspect traffic passively without impacting the network flow.
References:Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Interface Settings

質問: **83**
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. event viewer
B. dashboards
C. context explorer
D. reports
正解: **(**正解を表示します**)**

質問: **84**
ネットワーク管理者が月次の高度なマルウェアリスクレポートを確認している際に、CnC接続済みとしてリストされているホストに気づきました。このホストがマルウェアに感染しているかどうかをさらに確認するには、Cisco FMCのどこを調べればよいでしょうか？
A. 分析 > ホスト > 侵害の兆候
B. アナリスト > ファイル > マルウェアイベント
C. 分析 > ホスト > ホスト属性
D. 分析 > フライ > ネットワークファイル軌跡
正解: **(**正解を表示します**)**
To determine if a host is infected with malware, the network administrator can look at the Indications of Compromise (IOC) feature in Cisco FMC. The IOC feature analyzes network and endpoint data collected by Firepower sensors and AMP for Endpoints connectors, and identifies hosts that exhibit signs of compromise or infection. The IOC feature uses predefined rules based on Cisco Talos intelligence and other sources to detect IOCs on hosts. One of these rules is CnC Connected, which indicates that a host has communicated with a command-and-control (CnC) server that is known to be associated with malware activity2.
To view the IOC information for a host, the network administrator can navigate to Analysis > Hosts > Indications of Compromise in Cisco FMC, and select a host from the table. The IOC Details page will show the IOC events for that host, including the CnC Connected event, along with other information such as severity, timestamp, source, destination, protocol, and rule name. The network administrator can also view more details about each IOC event by clicking on it2.
The other options are incorrect because:
Analysis > Files > Malware Events shows information about files that have been detected as malware by Firepower sensors or AMP for Endpoints connectors. This does not show information about hosts that are infected with malware or have communicated with CnC servers3.
Analysis > Hosts > Host Attributes shows information about hosts that have been discovered by Firepower sensors, such as IP address, MAC address, operating system, applications, users, vulnerabilities, and so on. This does not show information about IOCs or CnC connections on hosts4.

Analysis > Files > Network File Trajectory shows information about files that have traversed your network and have been detected by Firepower sensors or AMP for Endpoints connectors. This allows you to track where a file came from, where it went, and what happened to it along the way. This does not show information about hosts that are infected with malware or have communicated with CnC servers5.

質問: **85**
エンジニアは、Cisco Secure Firewall Management Center (FMC) インベントリ内の Cisco Secure Firewall Threat Defense (FTD) ファイアウォールのモードを変更する必要があります。エンジニアは次のアクションを実行する必要があります。
* Secure FTD を Secure FMC に登録します。
* ファイアウォールモードを変更します。
* Secure FMC から Secure FTD デバイスの登録を解除します。
エンジニアは FTD に対してどのようなアクションを取る必要がありますか?
A. Secure FTD デバイスをリロードします。
B. 管理 IP アドレスを設定します。
C. コンソール ポートから Secure FTD CLI にアクセスします。
D. Secure FTD 設定を消去します
正解: **(**正解を表示します**)**
To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps:
Register the Secure FTD with Secure FMC.
Change the firewall mode.
Deregister the Secure FTD device from Secure FMC.
To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and manage the registration status of the FTD device.
Steps:
Connect to the Secure FTD device via the console port.
Access the CLI and execute the command to change the firewall mode (configure firewall-mode).
Deregister the device from FMC if needed.
Register or re-register the device with FMC as required.
References:Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Device Management and CLI Access.

質問: **86**

```
FMC: System > Monitor > [FTDv] > Advanced Troubleshooting > Capture w/Trace

1: 209.165.201.66.43410 > 209.165.202.100.8080: S 1349090467:1349090467(0) win
64240 <mss 1380,sackOK,timestamp 1421682252 0,nop,wscale 7>
 2: 209.165.202.100.8080 > 209.165.201.66.43410: R 0:0(0) ack 1349090468 win 0
 3: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425272499 0,nop,wscale 7>
 4: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
 admin prohibited filter
 5: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425273501 0,nop,wscale 7>
 6: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
 admin prohibited filter
 7: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425275617 0,nop,wscale 7>
 8: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
 admin prohibited filter
 9: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
 64240 <mss 1380,sackOK,timestamp 1425279677 0,nop,wscale 7>
10: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
11: 209.165.201.66.36438 > 209.165.202.143.8081: S 2008074308:2008074308(0) win
64240 <mss 1380,sackOK,timestamp 1425287869 0,nop,wscale 7>
12: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
13: 209.165.201.66.36438 > 209.165.202.143.8081: S 1804482258:1804482258(0) win
64240 <mss 1380,sackOK,timestamp 1425303997 0,nop,wscale 7>
14: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
15: 209.165.201.66.36438 > 209.165.202.143.8081: S 2230966104:2230966104(0) win
64240 <mss 1380,sackOK,timestamp 1425336509 0,nop,wscale 7>
16: 209.165.202.143 > 209.165.201.66 icmp: host 209.165.202.143 unreachable -
admin prohibited filter
```

図を参照してください。ユーザーは、さまざまな TCP ポートで多数の外部リソースに接続しようとします。ユーザーがポートを誤って入力すると、接続はすぐに閉じられ、接続が切断されるまでに 1 分以上かかります。エンジニアは、図に示すように、両方のタイプの接続をキャプチャすることに成功しました。
エンジニアは、2番目の接続グループのタイムアウト値を下げてユーザーの問題を解決するために、どのような設定を行う必要があるでしょうか？
A. ICMP プロトコル スイート全体を許可する送信アクセス ルール
B. 外部からの TCP リセット パケットを許可する受信アクセス ルール
C. リセット アクションでブロックする送信アクセス ルール
D. 外部からの ICMP タイプ 3 を許可する受信アクセス ルール
正解: **C** (コメントを発表する)

質問: **87**
エンジニアは、Cisco Secure Firewall Threat Defenseデバイスの内部インターフェースでSSHを許可する必要があります。現在、SSHは管理インターフェースでのみ許可されています。エンジニアはどのような種類のポリシーを設定する必要がありますか？
A. NATポリシー
B. プラットフォームポリシー
C. 侵入ポリシー
D. アクセス制御ポリシー

正解: **B** (コメントを発表する)

質問: **88**
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. 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
B. 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
C. 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。
D. 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
正解: **C** (コメントを発表する)

質問: **89**
エンジニアがCisco Secure Firewall Threat Defenseデバイスを設定している際に、新しいゼロデイ攻撃のデータペイロード内の特定のパターンを検出したことを理由に、新しい侵入ルールを作成するよう警告が表示されます。ルールの作成者と作成日を示す行を追加するには、どのキーワードタイプを使用する必要がありますか？
A. メタデータ
B. 内容
C. 参考
D. gtp_info
正解: (正解を表示します)
When creating a new intrusion rule in a Cisco Secure Firewall Threat Defense (FTD) device, the keyword type " metadata " must be used to add a line that identifies the author of the rule and the date it was created.
The metadata keyword is used to store additional information about the rule, such as authorship and creation date.
Steps:
In FMC, navigate toPolicies > Intrusion > Rules.
Create a new rule or edit an existing one.
Use the " metadata " keyword to add information about the author and date.
Example:
metadata: created_at 2023-06-15, author " John Doe " ;
By using the metadata keyword, you ensure that the rule contains relevant information for tracking its creation and authorship, which is essential for maintaining rule documentation and accountability.
References:Cisco Secure Firewall Management Center Intrusion Policy Guide, Chapter on Custom Rule Creation and Metadata Usage.

質問: **90**
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. サンドボックス分析
B. 動的解析
C. マルウェア分析
D. スペロ分析
正解: (正解を表示します)

質問: **91**
セキュリティ エンジニアは、1 つのサーバーへの UDP トラフィックをブロックする新しいポリシーを追加する必要があります。エンジニアは新しいオブジェクトを追加します。すべての UDP ポートを識別するために、エンジニアは次にどの操作を行う必要がありますか?
A. トランスポート番号を追加し、タイプとコードを指定します。
B. トランスポート プロトコルを指定し、ポート番号を空にします。
C. トランスポート プロトコルと必須のポート範囲を定義します。
D. UDP と TCP に対応する IP プロトコル番号を追加します。
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 **446**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
アクセス制御ポリシー内で使用されているオブジェクトを編集した後、どのアクションを実行する必要がありますか？
A. 使用中の既存のオブジェクトを削除します。
B. アクセスコントロールポリシーのCisco FMC GUIを更新します。
C. 更新された構成を再デプロイします。
D. 別のオブジェクト名を使用して別のルールを作成します。
正解: **C (**コメントを発表する**)**
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/reusable_objects.html

質問: **93**
セキュリティエンジニアが従業員の電子メールアドレスから疑わしいファイルを見つけ、分析のためにアップロードしようとしていますが、アップロードに失敗しています。最後の登録ステータスはまだアクティブです。この問題の原因は何ですか？
A. Cisco AMP forNetworksはCiscoThreat GridCloudに接続できません。
B. ホスト制限が設定されています。
C. ユーザーエージェントのステータスは監視するように設定されています。
D. Cisco AMP for Networksは、オンプレミスでCisco ThreatGridに接続できません。
正解: **(**正解を表示します**)**

質問: **94**
トラブルシューティングファイルを生成するために、Cisco FMC CLIでどのコマンドを入力しますか？
A. show running-config
B. show tech-support chassis
C. system support diagnostic-cli
D. sudo sf_troubleshoot.pl

正解: **C** (コメントを発表する)

質問: **95**
Cisco ISE と Cisco Secure Firewall Management Center の統合におけるレルムの役割は何ですか?
A. TACACS+ データベース
B. AD 定義
C. Cisco Secure Firewall VDC
D. (オプションが提供されていません - 確認または提供してください)
E. Cisco ISE コンテキスト
正解: **C** (正解を表示します)

質問: **96**
VPN 管理者は、Cisco Secure Firewall Management Center で管理されている Cisco Secure Firewall Threat Defense のインスタンスを、リモート アクセス VPN 認証に LDAP を使用するように変更しました。リモート ユーザーが VPN 経由で認証できるようにするには、どの証明書を追加する必要がありますか?
A. LDAPS サーバー証明書を Secure Firewall Management Center レルムに追加する必要があります。
B. Secure Firewall Threat Defense 証明書を LDAPS サーバーに追加する必要があります。
C. LDAPS サーバー証明書を Secure Firewall Threat Defense に
追加する必要があります。
D. Secure Firewall Management Center 証明書を LDAPS サーバーに追加する必要があります。
正解: **C** (コメントを発表する)

質問: **97**
エンジニアが、ペアの Cisco Secure Firewall デバイスのフェイルオーバー機能を展開しています。コア スイッチは、以前アクティブだったユニットの MAC アドレスを ARP テーブルに保持します。Cisco Secure Firewall のフェイルオーバー後もネットワーク ユーザーがインターネットにアクセスできるように、ダウンタイムを最小限に抑えるには、エンジニアはどの操作を行う必要がありますか?
A. 両方のユニットで同じ MAC アドレスを設定します。
B. 両方のユニットで仮想 MAC アドレスを使用します。
C. MAC アドレスをスイッチの ARP テーブルに追加します。
D. フェイルオーバー後に Gratuitous ARP を送信するスクリプトを実行します。
正解: **B** (コメントを発表する)

質問: **98**
管理者は、パッシブ ポート上の複数のスイッチから ERSPAN トラフィックを受信するようにトランスペアレントな Cisco FTD デバイスを設定していますが、FTD はトラフィックを処理していません。
A. ERSPAN トラフィックを処理するには、FTD をルーテッド モードにする必要があります。
B. スイッチには、GRE トラフィック伝送用の FTD デバイスへのレイヤ 3 接続がありません。
C. スイッチはモニタ セッション ID で設定されませんでした（ハットは FTD で定義されたフロー ID と一致します）
D. FTD はパッシブ ポートではなく、ERSPAN ポートで設定する必要があります。
正解: (正解を表示します)

質問: **99**
エンジニアは、トラフィックのホップ カウントを増やすことなく、単一のサブネット内のトラフィックを監視するようにファイアウォールを構成する必要があります。エンジニアはどのようにこれを達成しますか?
A. 侵入防止モードで Cisco Firepower をセットアップします。
B. Cisco Firepower をトランスペアレント ファイアウォールとして構成する
C. Cisco FDM によって管理されるように Cisco Firepower を設定します。
D. FXOS モニタ専用モードで Cisco Firepower を設定します。
正解: **B** (コメントを発表する)

質問: **100**
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 FMC Webブラウザー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 https:// < FMC IP > /capture/CAPI/pcap/test.pcap にアクセスすると、
PCAPファイルの代わりにエラー403 :アクセス禁止が表示されました。この問題を解決するために、エンジニアはどのような対応を取る必要がありますか？
A. HTTPSサーバーを無効にして、代わりにHTTPを使用してください。
B. デバイスプラットフォームポリシーでHTTPSサーバーを有効にします。
C. ブラウザのプロキシ設定を無効にします。
D. ブラウザのプロキシサーバー設定で、Cisco FTDのIPアドレスを使用します。
正解: (正解を表示します)

質問: **101**
エンジニアは、複数の Cisco FTD アプライアンスを設定 またはネットワークで使用）しています。複数のデバイス間でインターフェイスを使用するために Cisco FMC でインターフェイス オブジェクトを定義する際に、エンジニアが従わなければならない規則はどれですか?
A. インターフェイスは、セキュリティ ゾーンおよびインターフェイス グループに属することはできません
B. インターフェイス グループには複数のインターフェイス タイプを含めることができます
C. 2 つのセキュリティ ゾーンに同じインターフェイスを含めることができます
D. インターフェイス グループには、多くのデバイスからのインターフェイスを含めることができます。
正解: (正解を表示します)

質問: **102**
エンジニアがCiscoFTDデバイスをインストールし、ファイアウォールを通過する同じサブネット内のトラフィックを検査し、インターネット宛てのトラフィックを検査したいと考えています。
どの構成がこの要件を満たしますか？
A. IRBのみの透過ファイアウォールモード
B. ルーテッドインターフェイスのみのルーテッドファイアウォールモード
C. BVIおよびルーテッドインターフェイスを使用したルーテッドファイアウォールモード
D. 複数のBVIを備えた透過ファイアウォールモード
正解: (正解を表示します)

質問: **103**

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

質問: **104**
ネットワーク セキュリティ エンジニアは、高可用性ペアの障害のある Cisco FTD デバイスを交換する必要があります。障害のあるユニットを交換するときに、どの操作を行う必要がありますか?
A. 交換用ユニットの電源を入れる前に、アクティブな Cisco FTD デバイスをシャットダウンします。
B. 障害のある Cisco FTD デバイスが Cisco FMC に登録されたままであることを確認します。
C. 交換用ユニットの電源を入れる前に Cisco FMC をシャットダウンします。
D. 障害のある Cisco FTD デバイスを Cisco FMC から登録解除します。
正解: (正解を表示します)

質問: **105**
Cisco FTDには、BVIに割り当てられた2つの物理インターフェイスがあります。各インターフェイスは、同じスイッチ上の異なるVLANに接続されています。Cisco FTDがサポートするように設定されているファイアウォールモードはどれですか？
A. ルーティング
B. 高可用性クラスタリング
C. 透明
D. アクティブ/アクティブフェイルオーバー
正解: (正解を表示します)

質問: **106**
ネットワーク管理者が既存のFMCに新しいFTDを登録しました。管理者はFTDを透過モードに設定できません。透過モードを有効にするには、どの操作を実行すればよいでしょうか？
A. FMCからFTDデバイスの登録を解除し、CLI経由で透過モードを設定します。
B. 透過モードをサポートするFTDモデルを取得します。
C. 透過モードを設定する前に、FTD にブリッジ グループ インターフェイスを追加してください。
D. 2つの物理インターフェースにIPアドレスを割り当てます。
正解: **A** (コメントを発表する)

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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
ある企業が、Cisco FMCで管理されるCisco FTDを使用して侵入防止システムを導入する過程にある。
エンジニアは、潜在的な侵入を検知しつつ、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設定する必要があります。このタスクを達成するには、どの操作を実行すればよいでしょうか？
A. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプションのチェックを外して IPS モードを設定します。
B. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプションをオンにして、IDS モードを設定します。
C. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプションのチェックを外して IDS モードを設定します。
D. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプションをオンにして、IPS モードを設定します。
正解: **C** (コメントを発表する)

質問: **108**
セキュリティエンジニアが、複数の支店拠点向けにアクセス制御ポリシーを設定しています。これらの拠点は共通のルールセットを共有し、各拠点のローカルで有効な内部ネットワークサブネットを含むINSIDE_NETというネットワークオブジェクトを使用します。各拠点でポリシーの一貫性を維持しつつ、適用可能なルール内でローカルで有効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しょうか？
A. デバイスごとに固有のアクセス制御ポリシーを作成する
B. ポリシー継承の活用
C. 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
D. Cisco Talosから更新される動的なアクセス制御ポリシーを利用する
正解: (正解を表示します)

質問: **109**
単一の物理デバイス上の複数の論理デバイスが外部ホストにアクセスできるようにするには、Cisco Firepower に何を実装する必要がありますか?
A. 論理デバイスごとに VLAN サブインターフェースを定義します。
B. 同じモジュールから少なくとも 2 つのコンテナー インスタンスを追加します。
C. すべての論理デバイスに 1 つの共有管理インターフェイスを追加します。
D. すべての論理デバイス間のクラスタ制御リンクを設定します
正解: (正解を表示します)

質問: **110**
Cisco Threat Response を使用する場合、インテリジェンス サイクルのどの段階で調査結果が公開されますか?
A. 方向
B. 普及

C. 処理中
D. 分析
正解: **(**正解を表示します**)**
Disseminate: The dissemination phase publishes the results of the investigation or threat hunt. This information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

質問: **111**
ネットワークユーザーは、インターネットアクセスに断続的な問題が発生しています。エンジニアは、この問題がNATのリソース枯渇によって引き起こされていることを特定しました。エンジニアは、リソースが枯渇することなく、より多くのユーザーがインターネットにアクセスできるようにするには、動的NAT構成をどのように変更する必要がありますか？
A. 使用中のネットワークオブジェクトに対して追加の静的NATを定義します。
B. [詳細設定] タブで、インターフェース PAT へのフォールスルーを設定します。
C. 動的自動NATルールを動的手動NATに変換します。
D. ユーザーのオーバーフローを処理するために、ID NAT ルールを追加します。
正解: **B (**コメントを発表する**)**
Fallthrough to interface PAT is a feature that allows the dynamic NAT configuration to use the interface IP address as a last resort when the NAT pool is exhausted. This way, more users can access the internet without running out of resources. To enable this feature, the engineer must check the Enable PAT Fallback check box on the Advanced tab of the NAT rule editor1

質問: **112**
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. ファイアウォールバイパスを構成します。
B. 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。
C. CEO専用のNATポリシーを作成します。
D. CEOの信頼ポリシーを構成します。
正解: **(**正解を表示します**)**

質問: **113**
Cisco FTD デバイスがトランスペアレント ファイアウォール モードで設定されている場合、どの 2 つのインターフェイス タイプで IP アドレスを設定できますか？ （2つ選んでください。）
A. 診断
B. BVI
C. イーサチャネル
D. 物理
E. サブインターフェース
正解: **(**正解を表示します**)**

質問: **114**
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: **A,C** (コメントを発表する)
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: **115**
エンジニアは、内部ネットワークの IP アドレスが既知の悪意のあるホストと通信しているかどうかを検出するために、Cisco Secure Firewall Management Center で相関ポリシーを構成する必要があります。内部 IP アドレスによって行われた接続を追跡し、条件には外部の動的リストを使用する必要があります。エンジニアは、相関ポリシーでどのタイプのイベントを構成する必要がありますか?
A. 侵入影響アラート
B. マルウェア
C. 接続トラッカー
D. ネットワーク検出
正解: (正解を表示します)

質問: **116**
エンジニアが、Cisco Secure Firewall Threat Defense デバイスを、2 つのスイッチスタック間で透過モードで動作するように設定しています。両方のスイッチスタックで、インバンド管理に VLAN 10 が使用されています。ネットワークトラフィックを中断することなく、スイッチスタック間のトラフィックを検査するために、デバイス上で必要な 2 つの操作はどれですか？(2 つ選択してください。)
A. VLAN 10 用に BVI インターフェイスを設定します。
B. 少なくとも1つのブリッジグループを設定してください。
C. BPDUを事前検査から除外する。
D. ジャンボフレームをサポートするために、すべてのインターフェースでMTUを9198に設定します。
E. データトラフィックと管理トラフィック用に別々のルートを追加します。
正解: (正解を表示します)
Transparent firewall mode forwards traffic at Layer 2, so the participating physical interfaces must be assigned to at least one bridge group. This allows the device to inspect traffic while remaining logically transparent to the connected switch stacks. Bridge Protocol Data Units should also be exempted from advanced inspection. BPDUs are essential for spanning-tree operation, and delaying or blocking them during inspection restarts can produce topology instability or an interruption. A BVI provides Layer 3 addressing for device-originated traffic or management but is not inherently required merely to inspect transit traffic. Jumbo- frame configuration is unnecessary unless the network explicitly uses jumbo frames, and separate data and management routes do not establish transparent forwarding. Cisco specifically recommends using an EtherType ACL to trust BPDUs on each bridge-group member interface.
Cisco transparent firewall configuration

質問: **117**
エンジニアがCisco Secure Firewall Management Centerのマルチドメインインスタンスを設定しています。このインスタンスはCisco Secure Endpointと統合する必要があります。複数のドメインで同じIP-MACアドレスペアを持つホストを使用できるようにするには、エンジニアはどのような設定を行う必要がありますか？
A. グローバルドメイン
B. サブドメイン

C. セカンドレベルドメイン
D. リーフドメイン
正解: **D** (コメントを発表する)

質問: **118**
しばらくの間Firepowerを使用し、ネットワークとの相互作用について学習した後、管理者は悪意のあるアクティビティをユーザと関連付けようとしています。CiscoFirepowerダッシュボードでこの可視性を提供するには、どのウィジェットを設定する必要がありますか。
A. 相関イベント
B. 現在のセッション
C. カスタム分析
D. 現在の状況
正解: (正解を表示します)

質問: **119**
エンジニアは、特定のSGTのCiscoFirepowerの接続の問題を調査しています。エンジニアが64のSGTを使用してファイアウォールを通過する実際のパケットをキャプチャできるようにするコマンドはどれですか。
A. CAPヘッダーをキャプチャします-inline-tag 64 match ipanyanyとのみ入力します
B. CAPバッファ64をキャプチャします。
C. CAP match 64 type inline-tag ipanyanyをキャプチャします
D. CAPタイプをキャプチャするインラインタグ64 match ip any any
正解: (正解を表示します)

質問: **120**
高可用性の実行を一時的に停止するために、プライマリCisco FTDユニットのCLIで入力するコマンドはどれですか。
A. 高可用性レジュームを構成する
B. 高可用性の無効化を構成する
C. システムサポートネットワークオプション
D. 高可用性の一時停止を構成する
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: **121**
エンジニアは、組織のプライマリ Cisco FMC のディザスタ リカバリを提供する任務を負っています。プライマリ Cisco FMC に障害が発生した場合に元の企業ポリシーのコピーを利用できるようにするには、プライマリおよびセカンダリ Cisco FMC で何を行う必要がありますか?
A. プライマリ デバイスに障害が発生した場合、プライマリ Cisco FMC バックアップ構成をセカンダリ Cisco FMC デバイスに復元します。
B. プライマリとセカンダリの 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. プライマリとセカンダリの両方の Cisco FMC でハイ アベイラビリティを設定します。
D. アクティブな Cisco FMC 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。
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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
エンジニアがLANスイッチで作業していて、mime Cisco IPSへのネットワーク接続がダウンしていることに気づきました。トラブルシューティングの結果、スイッチが期待どおりに機能していると判断されました。この障害が発生するために何を実装する必要がありますか。
A. CiscoIPSが検出モードで設定されている
B. CiscoIPSはフェールオープンモードになるように設定されています
C. アップストリームルーターのルーティングプロトコルが正しく構成されていません
D. リンクステート伝播が有効になっている
正解: **(**正解を表示します**)**

質問: **123**
Cisco AMPプライベートクラウドの機能は何ですか？
A. パブリッククラウドへの直接接続を無効にします。
B. セキュリティインテリジェンスフィルタリングをサポートします。
C. 脅威インテリジェンスの匿名検索をサポートします
D. 動的解析を実行します
正解: **(**正解を表示します**)**

質問: **124**
分析用に設定された機密性の高いネットワークに関連するポートとプロトコルに関する情報をアナリストに提供するCiscoFMCレポートはどれですか。
A. ホストレポート
B. 火力レポート
C. マルウェアレポート
D. ネットワークレポート
正解: **(**正解を表示します**)**

質問: **125**
エンジニアは、Cisco FMC を介して Cisco FTD アプライアンスを展開し、ネットワーク セグメント全体に展開して、マルウェアと脅威を検出する必要があります。Cisco FTD インターフェイス モードを設定する場合、この要件を満たすアクション シーケンスはどれですか?
A. パッシブに設定し、侵入ポリシーとファイル ポリシーを定義してアクセス制御ポリシーを構成します。
B. none に設定し、事前フィルター ポリシーが定義されたアクセス コントロール ポリシーを構成します。
C. パッシブに設定し、プレフィルター ポリシーが定義されたアクセス コントロール ポリシーを構成します。
D. none に設定し、侵入ポリシーとファイル ポリシーが定義されたアクセス コントロール ポリシーを構成します。
正解: **A (**コメントを発表する**)**

質問: **126**
非同期ルーティング構成を展開するときに、同じインラインインターフェイスセットに複数のインラインインターフェイスペアを追加する利点は何ですか？
A. IPSがインバウンドトラフィックとアウトバウンドトラフィックを同じトラフィックフローの一部として識別できるようにします。
B. インターフェースは自動ネゴシエーションを無効にし、インターフェース速度はハードコードされて1000Mbpsに設定されます。
C. Snortプロセスの再起動中に、トラフィック検査を中断することなく続行できます。
D. インターフェイスは、メディアに依存しないインターフェイスクロスオーバーとして自動的に構成されます。
正解: **A (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601
/fpmc-config-guide-v60_chapter_01011010.pdf

質問: **127**
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. ファイアウォールでパケットキャプチャを実行する。
C. 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。
D. 管理者のPCでWiresharkを実行する
正解: **(**正解を表示します**)**

質問: **128**
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かどうかを判断するよう指示されました。このファイル検索を実行するには、どの2つの設定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. Cisco FMCにはSSL復号化ポリシーを含める必要があります。
B. Cisco FMC には、マルウェア検索のためのファイル検査ポリシーを含める必要があります。
C. Cisco FMC は FireAMP クラウド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Cisco AMP for Endpointsサービスに接続する必要があります。
正解: **(**正解を表示します**)**

質問: **129**
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. 監査
トリアージ
C. 保護
正解: **(**正解を表示します**)**
Reference: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints- deployment-methodology.html

質問: **130**
ネットワーク管理者はCiscoIPSアプライアンスを導入しており、トラフィックフローに影響を与えることなく最初に動作する必要があります。

また、データを収集して、不要なトラフィックをドロップするように再構成する前に、そのベースラインを提供する必要があります。これらの要件を満たすCiscoIPSモードはどれですか。
A. バイパス
B. 無差別
C. インラインタップ
D. フェイルセーフ
正解: **C** (コメントを発表する)

質問: **131**
Cisco FTDデバイスは、VTEPブリッジグループメンバーの入力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. UDPパケットタイプのみがサポートされています
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. VLANIDと宛先MACアドレスはオプションです
D. 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
正解: (正解を表示します)

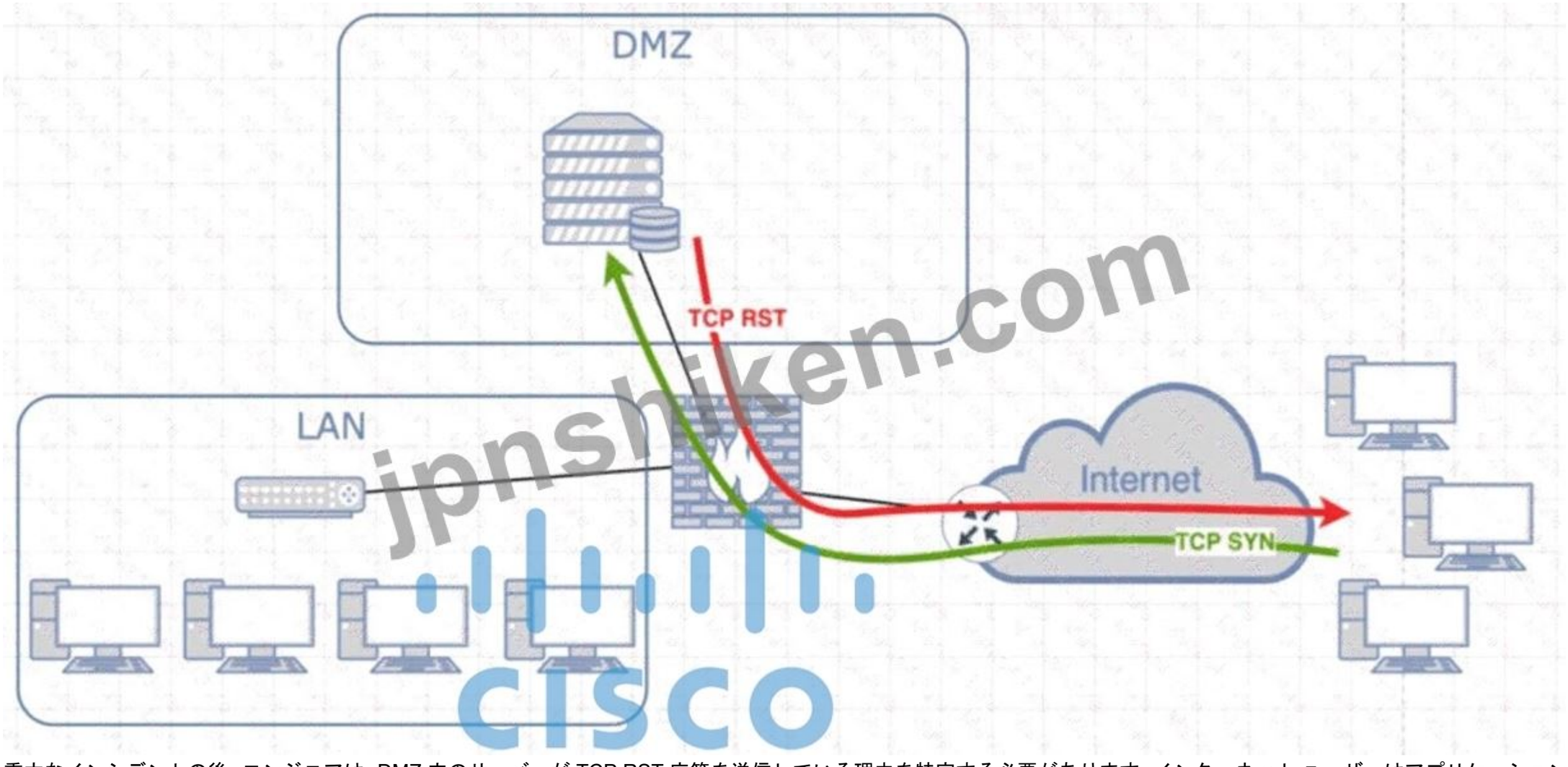
質問: **132**
展示資料を参照してください。
システム管理者がホストマシンからSCCMサーバーへの接続テストを実行したところ、サーバーから応答がありませんでした。pingパケットが宛先に到達し、ホストが応答を受信することを確実にするには、どの操作を行うべきでしょうか？
A. ICMP許可リストを作成し、ICMP宛先を追加して暗黙の拒否リストから削除します。
B. 検査後に ICMP トラフィックを許可するようにカスタム Snort シグネチャを設定します。
C. Snort ルールを変更して ICMP トラフィックを許可します。
D. ICMPトラフィックを許可するアクセス制御ポリシールールを作成します。
正解: (正解を表示します)

質問: **133**
Cisco Secure Firewall Management Center のリスク レポート機能の属性は何ですか?
A. マルチドメインシステム内のすべてのドメインを含む
B. マルチドメインシステムに現在のドメインを含める
C. 標準レポートで使用できる同じテンプレートを使用します
D. XML形式を使用してすべてのレポートをエクスポートします
正解: **B** (コメントを発表する)

質問: **134**
Cisco Secure Firewall Management Center で管理されているデバイスで、2 人のユーザーが同時に VPN ポリシーを変更すると、どのような結果になりますか?
A. 両方のユーザーがポリシーを編集でき、最後に保存された構成が保持されます。
B. 最初のユーザーがポリシーの編集を選択すると、構成がロックされます。
C. 両方のユーザーによる変更がポリシーにマージされます。

D. システムは、複数のユーザーによるポリシーの変更を防止します。
正解: (正解を表示します**)**
In Cisco Secure Firewall Management Center (FMC), when two users attempt to modify a VPN policy simultaneously, the system implements a locking mechanism to prevent conflicts. The first user who selects edit on the policy locks the configuration, preventing other users from making changes until the lock is released.
Steps:
When the first user selects edit on the VPN policy, FMC locks the policy for editing.
The lock ensures that only the first user can make changes.
Once the first user saves or cancels their changes, the lock is released.
Other users can then edit the policy.
This locking mechanism ensures that configuration conflicts are avoided and only one set of changes is applied at a time.
References:Cisco Secure Firewall Management Center Configuration Guide, Chapter on Policy Management and User Permissions.

質問: 135
図を参照してください。



重大なインシデントの後、エンジニアは、DMZ 内のサーバーが TCP RST 応答を送信している理由を特定する必要があります。インターネット ユーザーはアプリケーションにアクセスできますが、メインの Web ページを表示できません。エンジニアは、問題を特定して解決するために、どこでトラフィックをキャプチャする必要があるのでしょうか？

A. 境界ファイアウォールのインターネット接続インターフェース
B. 境界ルータの内部インターフェース
C. ISP ルータ
D. 境界ファイアウォールの DMZ インターフェース
正解: **D** (コメントを発表する)
The capture should be taken on the DMZ interface of the perimeter firewall because this is the firewall interface closest to the affected server. Capturing there shows the packets delivered to the server and the TCP RST packets returned by it. This placement helps determine whether the reset originates from the server, whether address translation changed the connection, or whether the firewall generated or altered the traffic.
Capturing only on the internet-facing interface would show the external behavior but provide less certainty about what reached or left the DMZ server. The perimeter router and ISP router are even farther from the suspected source. Cisco troubleshooting guidance recommends capturing as close as possible to the relevant endpoint and on the associated firewall data interface. List B's supplied answer C is therefore incorrect and has been corrected to D. Cisco firewall capture analysis

質問: **136**
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. 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。
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ルーテッド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. 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。
正解: **C** (コメントを発表する)
Reference:https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general- config/intro-fw.html

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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
エンジニアが、2台の新しいCisco Secure Firewall Threat Defenseアプライアンスを高可用性ペアとして構成しています。この高可用性ペアは、フェイルオーバーリンクの障害を検知し、より迅速にフェイルオーバーをトリガーする必要があります。
エンジニアはどの2つの設定値を下げなければならないか？(2つ選択してください。)
A. インターフェースのポーリング時間
B. ピアホールド時間
C. インターフェース故障限界
D. ピア投票時間
E. インターフェース保持時間
正解: **B,D** (コメントを発表する)
Peer poll time controls how frequently one high-availability unit sends hello or polling messages to determine whether its peer remains responsive. Peer hold time specifies how long the appliance waits without receiving the expected peer communication before declaring that peer unavailable. Decreasing both values causes the appliances to test peer availability more

frequently and wait less time before initiating failover. Interface- oriented timers are used to evaluate monitored data-interface failures and do not specifically accelerate detection of a failed failover link. Although shorter peer timers improve failover speed, excessively aggressive values can cause false failovers during congestion or high CPU utilization. Cisco explains that threat defense appliances monitor peer health through hello messages on the failover link and begin additional testing after consecutive messages are missed. Cisco Secure Firewall high-availability monitoring

質問: **138**

```
admin@Sourcefire3D:~$ cat /var/log/messages
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
 Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
 unsucessful: Failure when receiving data from the peer
```

図を参照してください。Cisco Secure Firewall Management Center 7.0 デバイスがインテリジェンスフィードの更新を受信できません。Cisco Secure Firewall Management Center は、SSL インスペクションを実行するプロキシ サーバーを使用するように構成されています。Cisco Secure Firewall Management Center デバイスがインテリジェンスフィードの更新をダウンロードできるようにするには、どの操作を実行すればよいでしょうか？

A. intelligence.sourcefire.com のプロキシサーバーに自己署名証明書をインストールします。

B. Cisco Secure Firewall Management Center デバイスでプロキシ認証が無効になっていることを確認してください。

C. プロキシサーバーがHTTPSを使用してインターネットと通信できることを確認します。

D. intelligence.sourcefire.com のプロキシ サーバーをバイパスします。

正解: **D** (コメントを発表する)

質問: **139**

ネットワーク管理者は、CiscoASAからCiscoFTDに移行しています。

EIGRPはCiscoASAで設定されていますが、CiscoFMCでは使用できません。

Cisco FTDでこの機能を有効にするには、管理者はどのアクションを実行する必要がありますか。

A. FlexConfigオブジェクトを使用してEIGRPパラメータを設定します。

B. FTDCLIを介してコマンド機能eigrpを追加します。

C. カスタム変数セットを作成し、変数セットで機能を有効にします。

D. FMCで高度な構成オプションを有効にします。

正解: (正解を表示します)

質問: **140**

セキュリティアナリストアカウントの権限を持つアナリストが相関イベントウィジェットを表示しようとしていますが、アクセスできません。しかし、他のダッシュボードにはアクセスできます。なぜこのようなことが起こるのでしょうか？

A. ウィジェットは Cisco FMC 内で設定されていません。

B. Cisco FMC内のAPI制限により、ウィジェットが表示されません。

C. ウィジェットは、アクティブなイベントが存在する場合にのみ表示されるように設定されています。

D. セキュリティアナリストの役割には、このウィジェットを表示する権限がありません。

正解: (正解を表示します)

質問: **141**
ネットワークエンジニアは、Cisco Secure Firewall Management Centerのコンソールから脅威イベントを監視する必要があります。エンジニアは、Cisco Secure Firewall Malware DefenseをSecure Firewall Management Centerに統合します。エンジニアは次にどのような操作を行う必要がありますか？
A. Secure Endpoint にログインし、[許可] をクリックして Secure Firewall Malware Defense と Secure FMC の接続を承認し、Secure FMC に Secure Firewall Malware Defense クラウド接続を追加し、Secure Endpoint 用に Secure Firewall Malware Defense クラウドを選択します。
B. Cisco Secure Endpointにログインし、[許可]をクリックしてSecure Firewall Malware DefenseとSecure FMCの接続を承認し、Secure Firewall Malware Defenseクラウド接続をSecure FMCに追加します。
C. Secure FMC で Secure Firewall Malware Defense クラウド接続を追加し、Secure Endpoint にログインして、[許可] をクリックして Secure Firewall Malware Defense と Secure FMC の接続を承認します。
D. Secure FMC で Secure Firewall Malware Defense クラウド接続を追加し、Secure Endpoint 用の Secure Firewall Malware Defense クラウドを選択し、Secure Endpoint にログインして、[許可] をクリックして Secure Firewall Malware Defense と Secure FMC の接続を承認します。
正解: **D** (コメントを発表する)

質問: **142**
エンジニアは、アクセス コントロール ポリシーの設定中に新しいルールを定義します。ポリシーを導入した後、ルールが期待どおりに機能せず、ルールに関連付けられているヒット カウンタがゼロを示しています。このエラーの原因は何ですか?
A. ルールは作成後に有効化されませんでした。
B. ルールで誤ったアプリケーション署名が使用されました。
C. Snort の間違ったソース インターフェイスがルールで選択されました。
D. ルールに対してロギングが有効になっていません。
正解: (正解を表示します)

質問: **143**
エンジニアは、Cisco Secure Firewall Threat Defense デバイス上でアクセス制御ポリシーを作成する必要があります。この会社には VoIP を多用するコンタクトセンターがあり、アクセス制御ポリシーの展開後にパフォーマンスの問題によってこのトラフィックが...されないことが重要です。VoIP トラフィックを処理するために、どのアクセス制御アクションルールを設定する必要がありますか？
A. モニター
B. 信頼
C. ブロック
D. 許可する
正解: **B** (コメントを発表する)
To ensure that VoIP traffic in a contact center is not impacted by performance issues after deploying an access control policy on a Cisco Secure Firewall Threat Defense (FTD) device, the engineer should configure the access control rule with the " trust " action. The " trust " action allows traffic to bypass inspection and policy enforcement, ensuring that critical VoIP traffic is not delayed or degraded.
Steps:
In FMC, navigate toPolicies > Access Control > Access Control Policy.
Create a new rule or edit an existing rule.
Set the source and destination for the VoIP traffic.
Set the action to " trust " to ensure the VoIP traffic is not inspected.
By configuring the rule with the " trust " action, the VoIP traffic will be prioritized, maintaining the quality and performance required for the contact center operations.

References:Cisco Secure Firewall Management Center Configuration Guide, Chapter on Access Control Policies and Traffic Management.

質問: **144**
IRB モードの Cisco FTD デバイスでダイナミック ルーティング プロトコルを実行するときに考慮すべき制限は何ですか?
A. リンクが古いルーティング プロトコルのみがサポートされます。
B. ディスタンス ベクトル ルーティング プロトコルのみがサポートされます。
C. EtherChannel インターフェイスのみが想定されます。
D. 非ブリッジインターフェイスのみがサポートされます。
正解: **(**正解を表示します**)**
Integrated routing and bridging (IRB) is a feature that allows you to route between different bridge groups on a Cisco FTD device. A bridge group is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. You can assign an IP address to a bridge group interface (BVI) and enable routing protocols on it, just like a regular routed interface. However, when you run a dynamic routing protocol on a Cisco FTD device in IRB mode, you can only use nonbridge interfaces as routing peers. You cannot use bridge group interfaces or bridge group member interfaces as routing peers2. This is because the routing protocol packets are sent and received on the nonbridge interfaces, and the bridge group interfaces are used only for forwarding data traffic3.

質問: **145**
エンジニアは、CiscoFMCでURLオブジェクトを定義する必要があります。SSLインスペクションを実行せずにURLを指定する正しい方法は何ですか？
A. サブジェクト共通名の値を使用します。
B. オブジェクトグループ内のすべてのサブドメインを指定します。
C. オブジェクトのプロトコルを指定します。
D. CRL配布ポイントからのすべてのURLを含めます。
正解: **(**正解を表示します**)**

質問: **146**
管理者は、QoS ポリシーを Cisco FTD 展開に追加しています。新しいルールがポリシーに追加され、QoS が 宛先インターフェース オブジェクト内のインターフェース」に適用されると、使用可能なインターフェース オブジェクトがありません。問題は何ですか?
A. QoS はルーテッド インターフェイスでのみ使用でき、このデバイスはトランスペアレント モードです。
B. QoS の追加を妨げている宛先インターフェース タイプ間に競合が存在します。
C. FTD は使用可能なリソースが不足しています。そのため、QoS を追加できません
D. インターフェイスが存在するネットワーク セグメントには、連続した IP 空間がありません。
正解: **(**正解を表示します**)**

質問: **147**
エンジニアは、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、非標準ポート 9443 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みているホストは、IP アドレス 10.20.10.20 です。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 D
D. オプション A
正解: **(**正解を表示します**)**

質問: **148**
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. CiscoFTDデバイスをCiscoASAポートチャネルに追加します。
B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **149**
Cisco FMC 管理者は、信頼できるネットワーク トラフィックの高速パスを設定して、パフォーマンスを向上させたいと考えています。管理者はどのタイプのポリシーでこの機能を構成しますか?
A. アイデンティティ ポリシー
B. 侵入ポリシー
C. ネットワーク分析ポリシー
D. プレフィルター ポリシー
正解: **D (**コメントを発表する**)**

質問: **150**
パケットをドロップできるインターフェイスタイプはどれですか。
A. passive
B. inline
C. ERSPAN
D. TAP
正解: **B (**コメントを発表する**)**
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring- firepower- threat-defense-int.html

質問: **151**
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クラスタリングモードで複数の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複数のCisco FTDHAペアを導入する
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、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。
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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**

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. IPSインラインリンク状態伝播を有効にする
B. 自動アプリケーションバイパスを有効にします。
C. SNORTエンジンが故障する前にプレフィルターポリシーを有効にします。
D. TrustALLアクセス制御ポリシーを設定します。
正解: **(**正解を表示します**)**

質問: **153**
エンジニアは接続の問題を調査する必要があり、Cisco FTDのパケットキャプチャ機能を使用することにした。
目的は、Cisco FTD デバイスを通過する実際のパケットを確認し、出力の一部として Snort の検出アクションを確認することです。capture-traffic コマンドを実行すると、パケットのみが表示されます。この問題を解決するには、どの操作を実行すればよいでしょうか？
A. Cisco FTD CLIではなく、Cisco FMC GUI内でトレースを実行します。
B. capture-traffic コマンドの一部として verbose オプションを使用します。
C. capture-traffic コマンドの後に -T オプションを使用してトレースを指定します。
D. キャプチャコマンドを使用し、トレースオプションを指定して必要な情報を取得します。
正解: **(**正解を表示します**)**

質問: **154**
ネットワーク管理者は、高可用性を確保するために、FMCに登録された新しいCisco Firepower 9300アプライアンス上にEtherChannelインターフェイスを作成する必要があります。管理者は、EtherChannelインターフェイスをどこに作成する必要がありますか？
A. FMC CLI
B. FTD CLI
C. FXOS CLI
D. FMC GUI
正解: **C (**コメントを発表する**)**
An EtherChannel interface is a logical interface that consists of a bundle of individual Ethernet links that act as a single network link. An EtherChannel interface can increase the bandwidth and reliability of a network connection5.
On a Cisco Firepower 9300 appliance registered with an FMC for high availability, the network administrator must create the EtherChannel interface on the FXOS CLI. The FXOS is the operating system that runs on the Firepower 9300 chassis and provides hardware management functions such as interface configuration, power supply status, fan speed control, and so on6.
To create an EtherChannel interface on the FXOS CLI, the network administrator can follow these steps5:
Connect to the FXOS CLI using SSH or console.
Enter scope eth-uplink command to enter Ethernet uplink mode.
Enter create port-channel command to create an EtherChannel interface.
Enter a port-channel ID (1-48) and a mode (on or active) for the EtherChannel interface.
Enter add interface command to add physical interfaces to the EtherChannel interface.
Enter one or more interface IDs (for example, 1/1) for the physical interfaces.
Enter commit-buffer command to save the changes.
The other options are incorrect because:

The FMC CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance. The FMC CLI is mainly used for managing FMC settings such as backup, restore, upgrade, troubleshoot, and so on7.
The FTD CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance. The FTD CLI is mainly used for managing FTD settings such as routing, NAT, VPN, access control, and so on8.
The FMC GUI does not provide any options to create an EtherChannel interface on a Firepower 9300 appliance. The FMC GUI is mainly used for managing FTD policies such as access control, intrusion, file, malware, and so on9.

質問: **155**
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. 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。
B. 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。
C. 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。
D. 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。
正解: **B (**コメントを発表する**)**

質問: **156**
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. システムサポートssl-client-hello-tuning
B. システムサポートssl-client-hello-display
C. システムサポートssl-client-hello-force-reset
D. システムサポートssl-client-hello-reset
正解: **(**正解を表示します**)**

質問: **157**
Cisco FMC を使用して迅速な脅威の封じ込めを実行するには、どのコンポーネントが必要ですか?
A. ISE
B. RESTful API
C. SIEM
D. DDI
正解: **(**正解を表示します**)**
To perform rapid threat containment with Cisco FMC, the necessary component is Cisco Identity Services Engine (ISE). ISE integrates with FMC to provide dynamic network access control and enforcement, allowing for quick isolation of compromised endpoints based on security events detected by FMC.
Steps:
* Integrate FMC with ISE by configuring the necessary settings in both platforms.
* Define security policies in FMC that trigger rapid threat containment actions via ISE.
* When a threat is detected, FMC can instruct ISE to isolate the affected endpoint, limiting its access to the network.
This integration enables automated and efficient threat containment, reducing the response time and mitigating the impact of security incidents.
References:Cisco Secure Firewall Management Center Integration Guide, Chapter on ISE Integration for Rapid Threat Containment.

質問: **158**
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. 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。
B. 外部NATIPアドレスが構成されていません。
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: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

質問: **159**
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. 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。
C. 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。
D. 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。
E. 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。
正解: **A,C (**コメントを発表する**)**
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Access_Control_Using_Intrusion_and_File_Policies.html

質問: **160**
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: **161**
ネットワーク管理者は、Cisco FTD の背後にあるルータにサイト間 IPsec VPN を設定しています。管理者は、UDP 500、4500 でこのデバイスへのトラフィックを許可するようにアクセス ポリシーを構成しましたが、ESP VPN トラフィックが機能していません。この問題を解決するアクションはどれですか?
A. インターフェイス PAT を使用するように NAT ポリシーを変更します。
B. アクセス ポリシーで IPsec インスペクションを有効にします。
C. すべてのポートを許可するようにアクセス ポリシーを変更します。
D. アクセス ポリシーの許可アクションを信頼に設定します。
正解: **(**正解を表示します**)**

質問: **162**

エンジニアが、現在のファイアウォールを置き換えるために、新しい Cisco Secure Firewall Threat Defense アプライアンスをセットアップしています。会社は、インライン セットを使用し、インライン セットの 1 つのインターフェイスがダウンすると、インライン セットの 2 番目のインターフェイスもダウンするように要求しています。展開要件を満たすために、エンジニアは何を構成する必要がありますか?
A. インライン タップ モード
B. 厳密な TCP 強制
C. リンク ステートの伝播
D. Snort フェイル オープン
正解: **(**正解を表示します**)**

質問: **163**
Cisco FTD 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)
A. BGPv6
B. 複数のインターフェイスにわたる最大 3 つの等コスト パスを使用した ECMP
C. 単一のインターフェイスにわたる最大 3 つの等コスト パスを使用した ECMP 【D】
: 透過ファイアウォール モードの BGPv4
D. ノンストップ転送を使用した BGPv4
正解: **A,C (**コメントを発表する**)**
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: **164**
2つのCiscoFTDデバイス間でハイアベイラビリティを実現するには、どの2つの条件を満たす必要がありますか。 2つ選択してください。）
A. 同じフラッシュメモリサイズ
B. 同じNTP構成
C. 同じDHCP / PPoE構成
D. 同じホスト名
E. 同数のインターフェース
正解: **B,E (**コメントを発表する**)**
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html Conditions In order to create an HA between 2 FTD devices, these conditions must be met:
Same model
Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal)) Same number of interfaces Same type of interfaces Both devices as part of same group/domain in FMC Have identical Network Time Protocol (NTP) configuration Be fully deployed on the FMC without uncommitted changes Be in the same firewall mode: routed or transparent.
Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.
Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis hostname navigate to FTD CLI and run this command

質問: **165**
エンジニアが、新しいCisco FTDデバイスの背後にあるホストからDNSサーバーへの接続に関するトラブルシューティングを行っている。

ホストはDMZ内のサーバーにDNSクエリを送信できません。エンジニアは、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ために、どのような対策を講じるべきでしょうか？
A. パケットトレーサーツールを使用して、パケットがどのホップでドロップされているかを特定します。
B. パケットキャプチャツールを使用して、トラフィックがどこでブロックされているかを確認し、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。
C. Threat Defense CLI ツールで show blocks コマンドを使用し、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. 接続イベントダッシュボードを使用してブロック理由を確認し、必要に応じて検査ポリシーを調整します。
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
446問、３０%ディスカウント、特別な割引コード: **JPNshiken**」