Cisco.300-710.v2026-06-26.q474

試験コード:	300-710
試験名称:	Securing Networks with Cisco Firepower
認定資格:	Cisco
無料問題数:	474
バージョン:	v2026-06-26
アクセス数:	139
ページビュー数:	4740
https://www.jpnpdf.com/Cisco.300-710.v2026-06-26.q474-mondaishu.html	

最新問題: **1**
Cisco FMC へのデバイスの削除と再追加に関する次の 2 つの記述のうち、正しいものはどれですか。(2 つ選択してください。)
A. 登録中に NAT および VPN ポリシーを再適用するオプションが用意されているため、ユーザーは登録が完了した後にポリシーを再適用する必要がありません。
B. Cisco FMC でデバイスを再度追加する前に、デバイスにマネージャを再度追加する必要があります。
C. Cisco FMC Web インターフェイスでは、デバイスを削除して再度追加するオプションは使用できません。
D. Cisco FMC Web インターフェイスは、ユーザーにアクセス制御ポリシーを再適用するように要求します。
E. 登録中に NAT および VPN ポリシーを再適用するオプションは利用できないため、ユーザーは登録が完了した後にポリシーを再適用する必要があります。
Answer: D,E (メーッセージを残す)
セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Device_Management_Basics.html

最新問題: **2**
Cisco FMCのイベントダッシュボードには、優先度の低い侵入ドロップイベントが大量に表示され、優先度の高いイベントが見過ごされています。エンジニアは、ポリシーを見直し、優先度の低いイベントを削減する任務を負っています。このタスクを達成するには、どのようなアクションを設定すればよいでしょうか？
A. パケットをドロップする
B. イベントを生成する
C. 接続を切断する
D. ドロップして生成
Answer: B (メーッセージを残す)
セクション: 展開
説明/参照:
参照" https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/working_with_intrusion_events.html

最新問題: **3**
ネットワーク管理者が月次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」と表示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のどこを確認す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 > ハエ > ネットワークファイルの軌跡
Answer: A (メーッセージを残す**)**
ホストがマルウェアに感染しているかどうかを判断するために、ネットワーク管理者はCisco FMCの侵害の兆候（IOC）機能を確認できます。IOC機能は、FirepowerセンサーとAMP for Endpointsコネクタによって収集されたネットワークおよびエンドポイントデータを分析し、侵害または感染の兆候を示すホストを特定します。IOC機能は、Cisco Talosインテリジェンスやその他のソースに基づく事前定義ルールを使用して、ホスト上のIOCを検出します。これらのルールの1つに「CnC接続」があります。これは、ホストがマルウェア活動に関連していることが知られているコマンドアンドコントロール（CnC）サーバと通信したことを示します2。
ホストのIOC情報を表示するには、ネットワーク管理者はCisco FMCで「分析」>「ホスト」>「侵害の兆候」に移動し、テーブルからホストを選択します。「IOC詳細」ページには、CnC接続イベントを含むそのホストのIOCイベントに加え、重大度、タイムスタンプ、送信元、宛先、プロトコル、ルール名などの情報が表示されます。ネットワーク管理者は、各IOCイベントをクリックすることで、より詳細な情報を表示することもできます2。
その他のオプションは、次の理由により正しくありません。
* 分析 > ファイル > マルウェアイベントでは、マルウェアとして検出されたファイルに関する情報が表示されます。
* FirepowerセンサーまたはAMP for Endpointsコネクタ。マルウェアに感染したホストやCnCサーバと通信したホストに関する情報は表示されません3。
* 「分析」>「ホスト」>「ホスト属性」では、Firepowerセンサーによって検出されたホストに関する情報（IPアドレス、MACアドレス、オペレーティングシステム、アプリケーション、ユーザー、脆弱性など）が表示されます。ただし、ホスト4上のIOCやCnC接続に関する情報は表示されません。
* 「分析」>「ファイル」>「ネットワークファイルトラジェクトリ」では、ネットワークを通過し、FirepowerセンサーまたはAMP for Endpointsコネクタによって検出されたファイルに関する情報が表示されます。これにより、ファイルの送信元、送信先、そしてその過程で何が起こったかを追跡できます。ただし、マルウェアに感染したホストやCnCサーバ5と通信したホストに関する情報は表示されません。

最新問題: **4**
エンジニアは、FTD 展開を通じてアプリケーション障害のトラブルシューティングを行っています。
FMC CLI の使用中に、問題のトラフィックが目的のポリシーと一致していないことが判明しました。これを修正するにはどうすればよいですか？
A. system support firewall-engine-dump-user-f density-data コマンドを使用してポリシーを変更し、アプリケーションがファイアウォールを通過できるようにします。
B. system support firewall-engine-debug コマンドを使用して、トラフィックがどのルールに一致しているかを判断し、それに応じてルールを変更します。
C. system support application-identification-debug コマンドを使用して、トラフィックがどのルールに一致するかを判断し、それに応じてルールを変更します。
D. システム サポート ネットワーク オプション コマンドを使用して、ポリシーを微調整します。
Answer: B (メーッセージを残す**)**

最新問題: **5**
ある企業は、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防止機能を導入しています。
速度と検出を優先する場合、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. 最大検出
B. セキュリティよりも接続性
C. 接続性よりもセキュリティを重視
D. バランスの取れたセキュリティと接続性
Answer: D (メーッセージを残す**)**

最新問題: **6**

Cisco Secure Firewall Threat Defenseデバイスは、インラインIPSモードで設定されており、インラインセット内のインターフェー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ることなく通過できるようにするには、インラインセット設定でどの設定を選択する必要がありますか？
A. タップモード
B. 厳格なTCP強制
C. リンク状態を伝播する
D. Snort フェイルオープン
Answer: D (メーッセージを残す)
インラインIPSモードでは、VDB（脆弱性データベース）アップデートの適用中にトラフィックが中断されることなく通過できるようにするため、「Short Fall Open」設定が必要です。この設定により、アップデート中や検査エンジンの障害など、検査プロセスに問題が発生した場合でも、トラフィックはファイアウォールを通過できます。
手順:
FMC で、インライン セット設定に移動します。
「Short Fall Open」オプションを有効にします。
設定を FTD デバイスに展開します。
これにより、更新中や検査プロセスでのその他の問題の発生時にネットワーク トラフィックが中断されることがなくなります。

最新問題: **7**
Cisco Firepower Threat Defense では、ルーテッド インターフェイスを設定するときに、どの 2 つのインターフェイス設定が必要ですか? (2 つ選択してください。)
A. 冗長インターフェース
B. イーサチャネル
C. スピード
D. メディアタイプ
E. デュプレックス
Answer: (解答を表示する)
説明
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm-interfaces.html

最新問題: **8**
エンジニアが2台目のCisco FMCをスタンバイデバイスとして設定しようとしていますが、アクティブユニットに登録できません。この問題の原因は何でしょうか？
A. 購入したライセンスには高可用性は含まれていません
B. 2 つのデバイス間の帯域幅は 10 Mbps しかありません。
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html
C. Cisco FMCデバイスで実行されているコードバージョンが異なります
D. プライマリ FMC には現在デバイスが接続されています。
Answer: (解答を表示する)

最新問題: **9**
管理者はネットワークをより適切にセグメント化するためにインターフェースオブジェクトを作成しようとしていますが、オブジェクトにインターフェースを追加する際に問題が発生しています。この失敗の原因は何ですか？
A. インターフェースは複数のネットワークの NAT に使用されています。
B. 管理者は複数のタイプのインターフェースを追加しています。

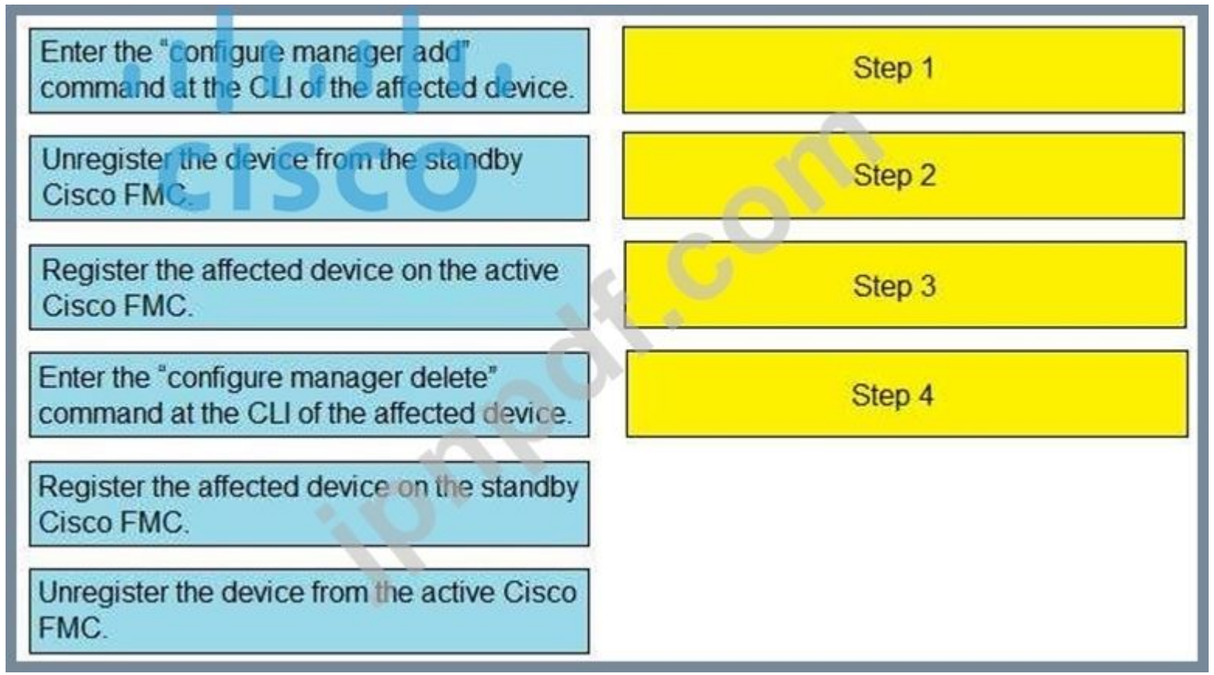
C. 管理者は複数のゾーンにあるインターフェースを追加しています。
D. インターフェースは複数のインターフェース グループに属しています。
Answer: D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4
インターフェース オブジェクト内のすべてのインターフェースは、すべて同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェース オブジェクトを作成した後は、含まれるインターフェースのタイプを変更することはできません。

最新問題: **10**

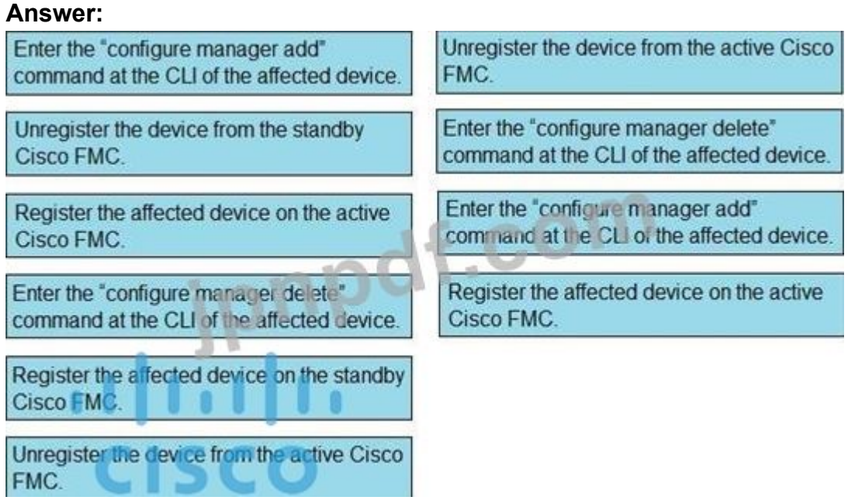
```
FMC: System > Monitor > [FTDv] > Advanced Troubleshooting > Capture w/Trace

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
```

展示をご覧ください。ユーザーは様々なTCPポートで多数の外部リソースへの接続を試みています。ポート番号を間違えると、接続は即座に切断され、切断されるまでに1分以上かかります。エンジニアは、展示に示すように、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。
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には、エンジニアは何を構成する必要がありますか?
A. 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
B. 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
C. 外部からのICMPタイプ3を許可する受信アクセスルール
D. 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
Answer: D (メーッセージを残す**)**

最新問題: **11**
ドラッグ＆ドロップ
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。
選択して配置:

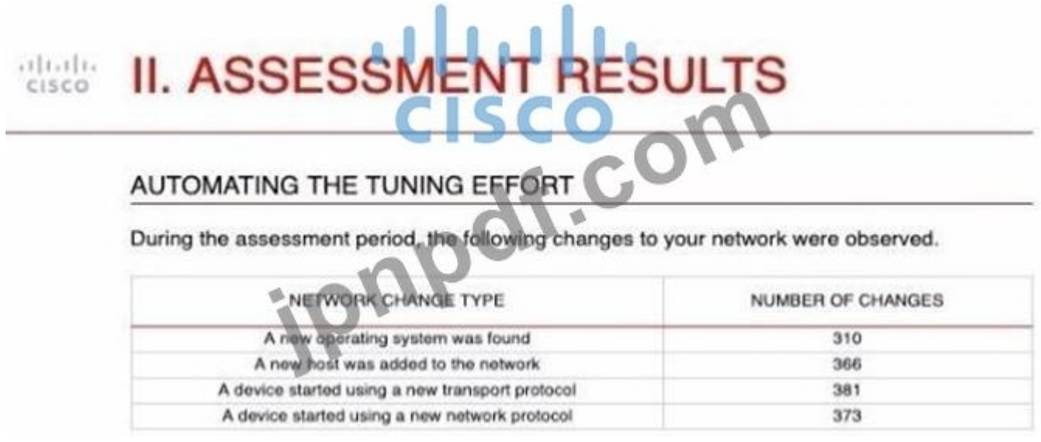


Answer:



セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_management_center_high_availability.html#id_32288

最新問題**: 12**
展示品を参照してください。



エンジニアは攻撃リスク レポートを分析し、ネットワーク上で 300 を超える新しいオペレーティング システムのインスタンスが確認されていることを発見しました。これらの新しいオペレーティング システムを保護するために、Firepower 構成はどのように更新されるのでしょうか。

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示します。

D. 管理者がポリシーを手動で更新します。

Answer: C (メーッセージを残す)

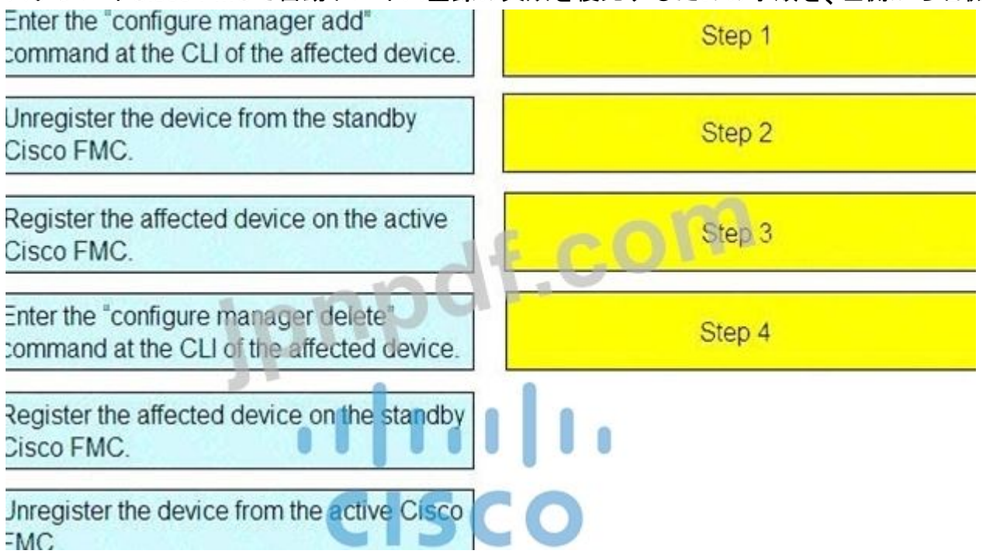
説明

参照:

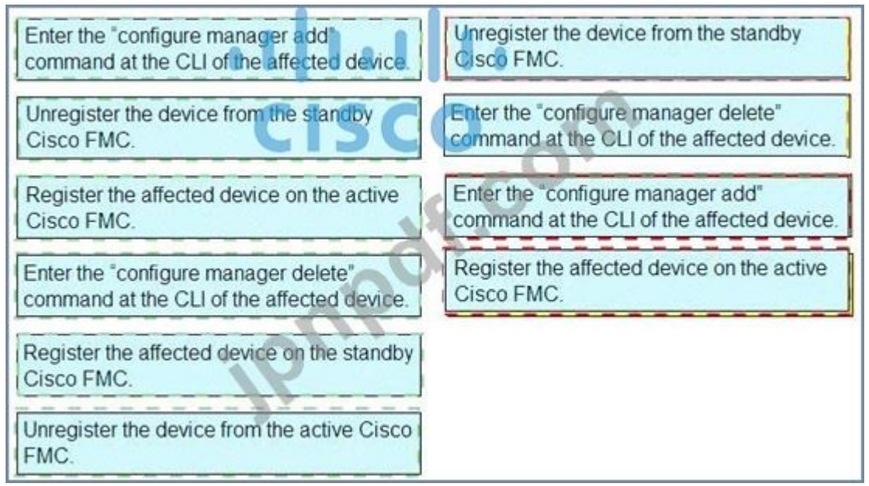
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailori

最新問題: 13

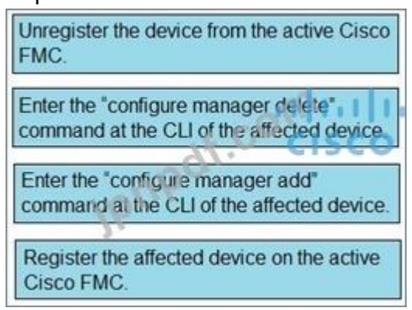
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。



Answer:



Explanation:



Explanation:

参考 :https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

最新問題**: 14**

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ースにわたる最大 3 つの等コスト パスを持つ ECMP

C. 単一インターフェース上で最大3つの等コストパスを持つECMP

D. 透過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備えたBGPv4

Answer: (解答を表示する**)**

セクション: 構成

説明/参照: 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

最新問題**: 15**

Cisco FTD クラスタリングを有効にするとどのような結果が得られますか?

A. 動的ルーティング機能では、マスター ユニットに障害が発生した場合、新しく選択されたマスター ユニットが既存のすべての接続を維持します。

B. マスター ユニットでは統合ルーティングおよびブリッジングがサポートされています。

C. サイト間 VPN 機能はマスター ユニットに制限されており、マスター ユニットに障害が発生するとすべての VPN 接続が切断されます。

D. すべての Firepower アプライアンスは Cisco FTD クラスタリングをサポートできます。
Answer: C (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

最新問題**: 16**
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、その情報を経営陣に送信するように依頼されています。このタスクを実行するにはどのようなメカニズムを使用する必要がありますか?
A. コンテキストエクスプローラー
B. ダッシュボード
C. レポート
D. イベントビューア
Answer: (解答を表示する**)**

最新問題**: 17**
Cisco FMC の迅速な脅威封じ込めにおいて脅威の詳細を交換するにはどのプロトコルが必要ですか?
A. SNMP v3
B. pxグリッド
C. 軍曹
D. BFD
Answer: B (メーッセージを残す**)**

最新問題**: 18**
エンジニアは、Secure Firewall Management Center アプライアンスで管理される Cisco Secure Firewall Threat Defense を設定しています。会社側は、リモートアクセス VPN ユーザーが社内ネットワークからアクセスできるようにしたいと考えています。要件を満たすには、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. NATポリシーの先頭にある手動NAT免除ルール
B. NATポリシーの下部にある手動NAT免除ルール
C. NATポリシーの先頭にある自動NAT免除ルール
D. NATポリシーの下部にある自動NAT免除ルール
Answer: A (メーッセージを残す**)**
最上部に配置された手動 (アイデンティティ) NAT 免除により、内部ネットワークと VPN クライアント プール間のトラフィックが変換されることがなくなり、リモート アクセス ユーザーが内部ホストからアクセスできるようになります。

最新問題**: 19**
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. coredump packet-engine を有効にする

B. キャプチャ
C. WORDをキャプチャする
D. キャプチャトラフィック
Answer: D (メーッセージを残す**)**

最新問題**: 20**
FTD ユニットにログインしたときに、ユニットがローカルで管理されているか、リモート FMC サーバーによって管理されているかを判断するために CLI で実行されるコマンドはどれですか。
A. システム生成トラブルシューティング
B. 設定セッションを表示
C. マネージャーを表示
D. 実行中の設定を表示 | マネージャを含める
Answer: C (メーッセージを残す**)**
セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/ b_Command_Reference_for_Firepower_Threat_Defense/c_3.html

最新問題**: 21**
エンジニアは、Cisco Secure Firewall Threat Defenseデバイスに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導入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影響を受けないようにすることが非常に重要です。VoIPトラフィックを処理するには、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. ブロック
B. 信頼
C. モニター
D. 許可する
Answer: (解答を表示する**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスにアクセス制御ポリシーを導入した後、コンタクトセンターのVoIPトラフィックがパフォーマンスの問題の影響を受けないようにするには、エンジニアはアクセス制御ルールに「信頼」アクションを設定する必要があります。「信頼」アクションにより、トラフィックは検査とポリシー適用をバイパスできるため、重要なVoIPトラフィックの遅延やパフォーマンス低下を防ぐことができます。
手順:
FMC で、[ポリシー] > [アクセス制御] > [アクセス制御ポリシー] に移動します。
新しいルールを作成するか、既存のルールを編集します。
VoIP トラフィックの送信元と宛先を設定します。
VoIPトラフィックが検査されないようにするには、アクションを「信頼」に設定します。
「信頼」アクションにより、VoIP トラフィックが優先され、コンタクト センターの運用に必要な品質とパフォーマンスが維持されます。

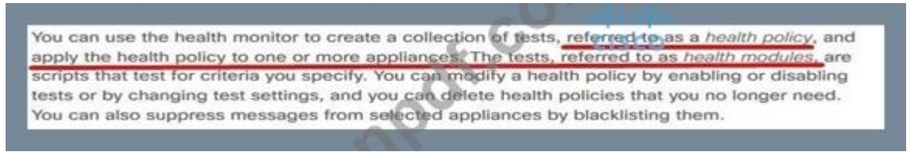
最新問題**: 22**
ネットワーク管理者が毎週のスケジュールされた攻撃リスクレポートを確認している際に、インパクト2の攻撃のフラグが付けられたホストに気づきました。このホストと攻撃に関するより詳細な情報を得るには、Cisco FMCのどこを確認すればよいでしょうか？
A. 分析 > ルックアップ > 全体
B. 分析 > 相関 > 相関イベント
C. 分析 > ホスト > 脆弱性
D. 分析 > ホスト > ホスト属性

Answer: C (メーッセージを残す)
説明
Cisco FMCの 「分析」> 「ホスト」> 「脆弱性」ページには、ネットワーク上のホストとそれらに関連する脆弱性に関する情報が表示されます。管理者は、ホストを影響レベルでフィルタリングできます。影響レベルは、ホストに対する攻撃が成功する可能性を示します。影響レベル2は、ホストが攻撃を受け、潜在的に脆弱であるものの、エクスプロイトは確認されていないことを意味します。管理者はホストをクリックすると、IPアドレス、オペレーティングシステム、アプリケーション、プロトコル、侵入イベントなどの詳細を表示できます。また、各脆弱性のCVE ID、説明、重大度、推奨アクションなどの詳細も確認できます。

最新問題: **23**
Cisco FirePOWER センサーを Firepower Management Center に登録するにはどの CLI コマンドを使用しますか?
A. システムを構成して <ホスト><キー> を追加します
B. マネージャーを設定 <キー> ホストを追加
C. マネージャーの削除を構成する
D. configure manager add <ホスト><キー>
Answer: (解答を表示する)
http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.html

最新問題: **24**
ネットワーク管理者が先月のファイルレポートを確認したところ、exeファイルを除くすべてのファイルタイプが 「不明」と表示されていることに気づきました。この問題の原因は何でしょうか？
A. Spero ファイル分析のみが有効になります。
B. Cisco FMC はインターネットに接続できず、ファイルを分析できません。
C. マルウェア ライセンスが Cisco FTD に適用されていません。
D. アクセス ポリシーにファイル ポリシーが適用されていません。
Answer: C (メーッセージを残す)

最新問題: **25**
Cisco Firepower Management Center では、管理対象デバイスからヘルス モジュール アラートを収集するために使用されるポリシーはどれですか。
A. 健康政策
B. システムポリシー
C. 相関ポリシー
D. アクセス制御ポリシー
E. 健康意識向上政策
Answer: A (メーッセージを残す)



最新問題: **26**
Cisco Security Analytics と Logging を使用してファイアウォールからの集約されたログ データにアクセスして表示するには、どの 2 つのソリューションを使用しますか? (2 つ選択してください。)
A. シスコ ディフェンス オーケストレータ
B. セキュアクラウド分析

C. シスコ セキュア ネットワーク アナリティクス
D. シスコ プライム インフラストラクチャ
E. シスコ Catalyst センター
Answer: B,C (メーッセージを残す)

最新問題**: 27**
エンジニアは、サードパーティ製のセキュリティインテリジェンスツールを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で動作しており、メモリは8GB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サーバーを追加する
Answer: A,C (メーッセージを残す)
Threat Intelligence Director (TID) を使用してサードパーティのセキュリティ インテリジェンス フィードを Cisco Secure Firewall Management Center (FMC) と統合するには、次のアクションが必要です。
バージョン 6.6 にアップグレード: Threat Intelligence Director をサポートするには、FMC が少なくともバージョン 6.6 を実行している必要があります。
バージョン 6.2.3 では、この統合に必要な機能はサポートされていません。
TAXIIサーバのURLを追加 :Threat Intelligence Directorは、TAXII（Trusted Automated eXchange of Indicator Information）を使用して、サードパーティのソースから脅威インテリジェンスデータを取得します。TAXIIサーバのURLをFMCのTID設定に追加する必要があります。
手順:
FMC をバージョン 6.6 以降にアップグレードします。
FMC で、[統合] > [脅威インテリジェンス ディレクター] に移動します。
TAXII サーバーの URL を入力して、新しい TAXII サーバーを追加します。
これらのアクションにより、サードパーティの脅威インテリジェンス フィードとの統合が可能になり、FMC のセキュリティ機能が強化されます。
参考資料:Cisco Secure Firewall Management Center 管理者ガイド、Threat Intelligence Director の章。

最新問題**: 28**
ある組織では、現在のファイアウォールを置き換えるために 2 つの新しい Cisco FTD デバイスをセットアップしており、ネットワークのダウンタイムは許されません。セットアップ プロセス中に、2 つのデバイス間の同期が失敗します。この問題を解決するには、どのようなアクションが必要ですか?
A. 両方のデバイスが同じタイプのインターフェースで構成されていることを確認します
B. 両方のデバイスのポートチャネル番号が同じであることを確認します。
C. 両方のデバイスのフラッシュメモリサイズが同じであることを確認します
D. 両方のデバイスが同じソフトウェアバージョンを実行していることを確認します
Answer: D (メーッセージを残す)

最新問題**: 29**
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 マルウェア防御を Secure Firewall Management Center に統合します。次に、エンジニアはどのようなアクションを実行する必要がありますか？
A. Secure FMC で Secure Firewall Malware Defense クラウド接続を追加し、Secure Endpoint 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、Secure Firewall Malware Defense から Secure FMC への接続を承認します。

B. 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、Secure Firewall Malware Defense から Secure FMC への接続を承認します。
C. Cisco Secure Endpoint にログインし、[許可] をクリックして、Secure Firewall Malware Defense から Secure FMC への接続を承認し、Secure Firewall Malware Defense クラウド接続を Secure FMC に追加します。
D. Secure Endpoint にログインし、[許可] をクリックして Secure Firewall Malware Defense から Secure FMC への接続を承認し、Secure Firewall Malware Defense クラウド接続を Secure FMC に追加して、Secure Endpoint の Secure Firewall Malware Defense クラウドを選択します。
Answer: B (メーッセージを残す**)**
Cisco Secure Firewall Malware Defense を Secure Firewall Management Center (FMC) と統合した後、次に必要な手順は、FMC に Malware Defense クラウド接続を追加することです。
次に、エンジニアは、Secure Endpoint から [許可] をクリックして接続を承認する必要があります。
この 2 段階のプロセスにより、FMC での脅威イベントの適切な同期と可視性が確保されます。

最新問題**: 30**
Cisco Firepower Management Center CLI ではどのコマンドライン モードがサポートされていますか?
A. ユーザー
B. 管理者
C. 構成
D. 特権
Answer: C (メーッセージを残す**)**

最新問題**: 31**
有効な Cisco AMP ファイルの性質とは何ですか?
A. 悪意のない
B. マルウェア
C. 正常動作
D. 純粋
Answer: B (メーッセージを残す**)**
セクション: 統合
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Reference_a_wrapper_Chapter_topic_here.html

最新問題**: 32**
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。
Answer: (解答を表示する**)**
「ルーティングされたファイアウォール モードでは、アクセス ルールで許可されていても、ブロードキャスト トラフィックとマルチキャスト トラフィックはブロックされます...」
「ブリッジ グループは CDP パケットを通過させません...」
https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913- general-config/intro-fw.html

最新問題**: 33**
ネットワーク エンジニアは、別の IP サブネットを作成せずにトラフィック検査のために FTD デバイスを介してユーザー セグメントを拡張しています。これは、ルーティング モードの FTD デバイスでどのように実現されるのでしょうか。
A. ARPを利用してトラフィックをファイアウォールに誘導する
B. インラインセットインターフェースを割り当てることによって
C. BVIを使用して、ユーザーセグメントと同じサブネットにBVI IPアドレスを作成します。
D. 事前フィルタルールを活用してプロトコル検査をバイパスする
Answer: C (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

最新問題**: 34**
CIO は、ネットワーク管理者に、上位 DNS クエリの URL カテゴリ統計と URL レピュテーション統計のカスタム分析テーブルを表示するダッシュボードを経営陣に提示するよう依頼します。
管理者は、この情報を経営陣向けに迅速に作成するため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. 攻撃レポートを実行し、DNS でフィルターしてこの情報を表示します。
B. 侵入イベントのダッシュボード タブをコピーし、各ウィジェットを変更して正しいグラフを表示します。
C. 接続イベント ダッシュボードを変更して、管理用のビューに情報を表示します。
D. 新しいダッシュボードを作成し、必要なテーブルを指定する 3 つのカスタム分析ウィジェットを追加します。
Answer: D (メーッセージを残す**)**

最新問題**: 35**
どの Cisco Firepower ルール アクションが HTTP 警告ページを表示しますか?
A. ブロック
B. インタラクティブブロック
C. モニター
D. 警告付きで許可
Answer: B (メーッセージを残す**)**

最新問題**: 36**
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。エンジニアが次のURLにアクセスした場合：
..<FMC IP>/capture/CAP/pcap/sample.pcap
エンジニアがPCAPファイルではなく「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うすればよいですか？
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 ブラウザーのプロキシ設定を無効にします。
Answer: (解答を表示する**)**
エンジニアがCisco Secure Firewall Management Center（FMC）からパケットキャプチャファイルをダウンロードしようとした際に「403: Forbidden」エラーが発生した場合、デバイスプラットフォームポリシーでHTTPSが有効になっていないことが原因である可能性があります。この問題を解決するには、エンジニアがプラットフォームポリシーでHTTPSを有効にする必要があります。
手順:
* FMC で、[ポリシー] > [デバイス管理] > [プラットフォーム設定] に移動します。
* 関連するプラットフォーム ポリシーを編集します。
* デバイスで HTTPS を有効にします。
*変更を FTD デバイスに展開します。
これにより、FMC および FTD デバイスはパケット キャプチャ ファイルを HTTPS 経由で安全に転送できるようになり、403 エラーが解決されます。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、プラットフォーム設定と HTTPS 構成の章。

最新問題**: 37**
Cisco FTD のブリッジ グループ インターフェイスに関する次の 2 つの記述のうち正しいものはどれですか。(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存在する必要があります。
B. ブリッジ グループは、透過型ファイアウォール モードとルーティング型ファイアウォール モードの両方でサポートされます。
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. ブリッジ グループ メンバーを使用する場合、双方向転送検出エコー パケットは 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。
Answer: C,D (メーッセージを残す**)**
参考: 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

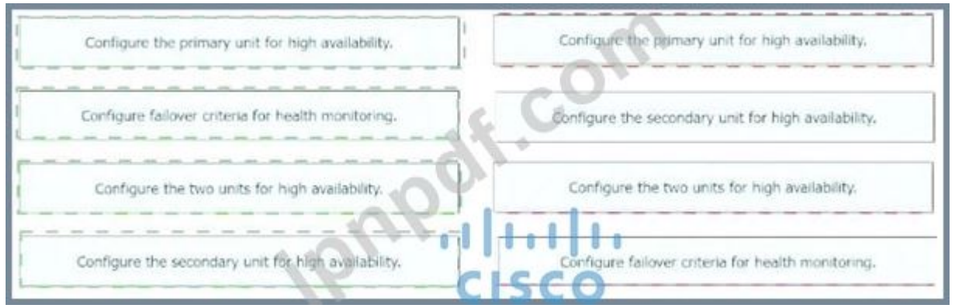
最新問題**: 38**
Cisco Secure Client 経由で Cisco Secure Firewall Threat Defense デバイスの背後にある企業ネットワークに接続しているリモートユーザーから、ソフトフォンを使用してリモートユーザー間で通話する際に音声が聞こえないという報告があります。同じユーザーが企業ネットワーク内の社内ユーザーには問題なく通話できます。この問題の原因は何ですか？
A. ヘアピニング機能はCisco Secure Firewall Threat Defenseでは利用できません
B. Cisco Secure Firewall Threat Defenseには、外部から外部への通信を許可するNATポリシーが必要です。
C. Cisco Secure Firewall Threat Defenseでハブ経由のスポーク間接続を有効にするオプションが選択されていません
D. Cisco Secure Firewall Threat Defenseのリモートアクセスvpnでスプリットトンネリングが有効になっています
Answer: B (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client- v4x/220337-troubleshoot-common-anyconnect-communica.html

最新問題**: 39**
ネットワーク管理者は、Cisco Secure Firewall Management Center に登録された透過型 Cisco Secure Firewall Threat Defense を設定しようとしています。管理者は、ブリッジグループの 2 つのインターフェース間で ARP トラフィックを通過させるように、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. デバイスのデフォルト設定を使用します。
B. 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。

C. ARP 検査を無効にする必要があります。
D. アクセス ポリシーは MAC アドレス FFFF.FFFF.FFFF を許可する必要があります。
Answer: A (メーッセージを残す**)**
デフォルトでは、すべての ARP パケットはブリッジ グループ内で渡されます。
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/device-ops-tfw.html

最新問題**: 40**
エンジニアは、2台のCisco Secure Firewall Threat Defenseアプライアンスに高可用性を設定する必要があります。設定手順を左側から右側のシーケンスにドラッグ＆ドロップしてください。

Answer:



Explanation:
ステップ1（プライマリユニットを高可用性用に構成する）、
ステップ2（セカンダリユニットを高可用性用に構成する）
ステップ3（2つのユニットを高可用性用に構成する）、
ステップ4（ヘルスモニタリングのフェイルオーバー基準を構成する）

最新問題**: 41**
ネットワーク管理者は、Cisco Secure Firewall Management Center に登録された透過型 Cisco Secure Firewall Threat Defense を設定しようとしています。管理者は、ブリッジグループの 2 つのインターフェース間で ARP トラフィックを通過させるように、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. ARP 検査を無効にする必要があります。

D. 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。
Answer: B (メーッセージを残す**)**

最新問題**: 42**
エンジニアは、実IPアドレスをファイアウォールの背後に隠したまま、Cisco Secure Firewall Thread DefenseをCisco Secure Firewall Management Centerに追加したいと考えています。エンジニアは、Cisco Secure Firewall Thread Defenseでconfigure manager add Cisc0497926642コマンドを設定しました。
コマンドを追加しても、デバイスがCisco Secure Firewall Management Centerに追加されません。このタスクを実行するには、設定コマンドにどの設定を追加する必要がありますか？
A. NAT ID
B. 登録キー
C. Cisco FTD IPアドレス
D. 解決しない
Answer: (解答を表示する**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスがNATの背後にあり、実IPアドレスが隠されている場合、configure manager addコマンドでNAT IDを使用する必要があります。これにより、FMCはNATトラバーサルを介してFTDデバイスを一意に識別し、通信を確立できます。NAT IDがない場合、登録は失敗します。

最新問題**: 43**
管理者がCisco Secure Firewall Management Center内の保存済み検索に基づいて新しいレポートテンプレートを設定しようとしています。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、ベースには別の種類の保存済み検索を使用する予定です。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点は何でしょうか？
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. 保存した検索は、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利用できます。
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。
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Management Center（FMC）で保存した検索条件に基づいて新しいレポートテンプレートを設定する場合、保存した検索条件は作成に使用したレポートテンプレートに固有のものであることにご注意ください。保存した検索条件は、異なるレポートテンプレート間で自由に使用することはできません。
異なる種類の保存済み検索を使用するには、その検索が使用している特定のレポートテンプレートと一致していることを確認する必要があります。この制限により、保存済み検索パラメータがレポートのデータ要件と一致することが保証されます。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、レポートと保存された検索の章。

最新問題**: 44**
エンジニアがCisco Secure Firewall Threat Defenseデバイスを設定している際に、新たなゼロデイエクスプロイトのデータペイロードに特定のパターンが検出されたため、新しい侵入ルールを作成するように警告されました。ルールの作成者と作成日を識別する行を追加するには、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. コンテンツ
C. 参照
D. gtp_info
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスで新しい侵入ルールを作成する場合、キーワードタイプ
ルールの作成者と作成日を識別する行を追加するには、「metadata」を使用する必要があります。metadataキーワードは、作成者や作成日など、ルールに関する追加情報を保存するために使用されます。
手順:

* FMC で、[ポリシー] > [侵入] > [ルール] に移動します。
* 新しいルールを作成するか、既存のルールを編集します。
* 「metadata」キーワードを使用して、作成者と日付に関する情報を追加します。
例：
メタデータ: created_at 2023-06-15、作成者 「John Doe」;
メタデータ キーワードを使用すると、ルールの作成と作成者を追跡するための関連情報がルールに含まれることが保証されます。これは、ルールのドキュメントと説明責任を維持するために不可欠です。
参考資料: Cisco Secure Firewall Management Center 侵入ポリシー ガイド、カスタム ルールの作成とメタデータの使用に関する章。

最新問題**: 45**
エンジニアは、Cisco Secure Firewall Threat Defenseデバイスに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、このトラフィックがアクセス制御ポリシーの導入後にパフォーマンスの問題によって影響を受けないようにすることが非常に重要です。VoIPトラフィックを処理するには、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
Answer: (解答を表示する**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスにアクセス制御ポリシーを導入した後、コンタクトセンターのVoIPトラフィックがパフォーマンスの問題の影響を受けないようにするには、エンジニアはアクセス制御ルールに 「信頼」アクションを設定する必要があります。 「信頼」アクションにより、トラフィックは検査とポリシー適用をバイパスできるため、重要なVoIPトラフィックの遅延やパフォーマンス低下を防ぐことができます。
手順:
* FMC で、[ポリシー] > [アクセス制御] > [アクセス制御ポリシー] に移動します。
* 新しいルールを作成するか、既存のルールを編集します。
* VoIP トラフィックの送信元と宛先を設定します。
* VoIP トラフィックが検査されないようにするには、アクションを 「信頼」に設定します。
「信頼」アクションでルールを構成すると、VoIP トラフィックが優先され、コンタクト センターの運用に必要な品質とパフォーマンスが維持されます。
参考資料: Cisco Secure Firewall Management Center 構成ガイド、アクセス制御ポリシーとトラフィック管理の章。

最新問題**: 46**
エンジニアがconfigure manager add <FMC IP> Cisc404225383コマンドを使用して、新しいCisco FTDデバイスをCisco FMCに追加しようとしましたが、デバイスが追加されません。なぜこのような現象が発生するのでしょうか？
A. コマンドにDONOTRESOLVEを追加する必要があります
B. コマンドに登録キーがありません
C. Cisco FMCはNATデバイスの背後にあるため、NAT IDが必要です。
D. 使用するIPアドレスはCisco FMCではなくCisco FTDのIPアドレスである必要があります。
Answer: (解答を表示する**)**

最新問題**: 47**
エンジニアはCisco TACに確認してもらうため、Cisco FTDセンサーの設定を取得しようとしましたが、デバイスのCUに直接アクセスできません。デバイスのCLIは、エンジニアがアクセスできるCisco FMCによって管理されています。Cisco FMCのどのアクションが、デバイスのCLIへのアクセスを許可しますか？
A. Cisco FMC 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。
B. Cisco FMC 内の設定のバックアップを作成します。
C. Cisco FMC 内の Cisco FTD CLI 機能で show run all コマンドを使用します。
D. Cisco FMC のファイル ダウンロード セクション内で設定ファイルをダウンロードします。
Answer: (解答を表示する**)**
Cisco FMCでは、エンジニアはCisco FTDセンサーのCLIへのアクセスを許可するために、Cisco FTD CLI機能内から 'show run」コマンドを使用できます。このコマンドを使用すると、エンジニアはCisco FTDセンサーの現在の設定（前回の設定保存以降に加えられた変更を含む）を確認できます。エンジニアは、トラブルシューティングやサポートのために必要に応じて、この設定をCisco TACと共有できます。

最新問題**: 48**
ネットワークセキュリティ侵害が発生した後、エンジニアは企業ネットワークのセキュリティを強化する必要があります。経営陣には、発生しているネットワーク脅威の概要を定期的に報告する必要があります。エンジニアは、Cisco Secure Firewall Management Center から必要なデータを閲覧するために、経営陣にどのようなアクセス権限を与える必要がありますか？
A. 優先度と分類によるイベントと1日のスライド時間枠の設定
B. セキュリティ インテリジェンス統計ダッシュボードの [最終表示] オプションが 1 日に設定されています
C. ネットワークリスクレポートテンプレートに基づいて生成される毎日の定期タスクを含むレポート
D. 分析 > 1日のスライディングタイムウィンドウによるステータス
Answer: C (メーッセージを残す**)**

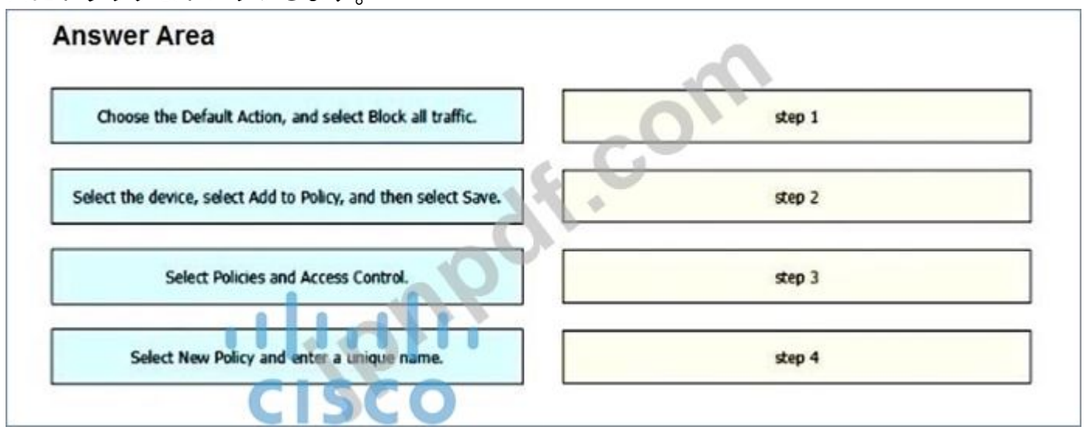
最新問題**: 49**
エンジニアは、内部ネットワークの IP アドレスが既知の悪意のあるホストと通信したことを検知するために、Cisco Secure Firewall Management Center で相関ポリシーを設定する必要があります。
内部IPアドレスによる接続を追跡し、条件には外部動的リストを使用する必要があります。エンジニアは相関ポリシーでどのタイプのイベントを設定する必要がありますか？
A. ネットワーク検出
B. マルウェア
C. 接続トラッカー
D. 侵入影響アラート
Answer: C (メーッセージを残す**)**
内部IPアドレスが外部の動的リストを使用して既知の悪意のあるホストへの接続を開始したことを検出するには、相関ポリシーで接続トラッカーイベントを設定する必要があります。これにより、ポリシーはトラフィックフローを監視し、外部の脅威インテリジェンスソースと相関させることができます。

最新問題**: 50**
ネットワーク管理者は、Cisco FTD デバイスの背後でホストされている Web サイトへのアクセスのトラブルシューティングを行っています。外部クライアントは、HTTPS 経由で Web サーバーにアクセスできません。Web サーバーに設定されている IP アドレスは 192 168 7.46 です。管理者は、コマンド capture CAP interface outside match ip any 192.168.7.46 255.255.255.255 を実行していますが、キャプチャでトラフィックを確認できません。なぜこのようなことが起こるのでしょうか。

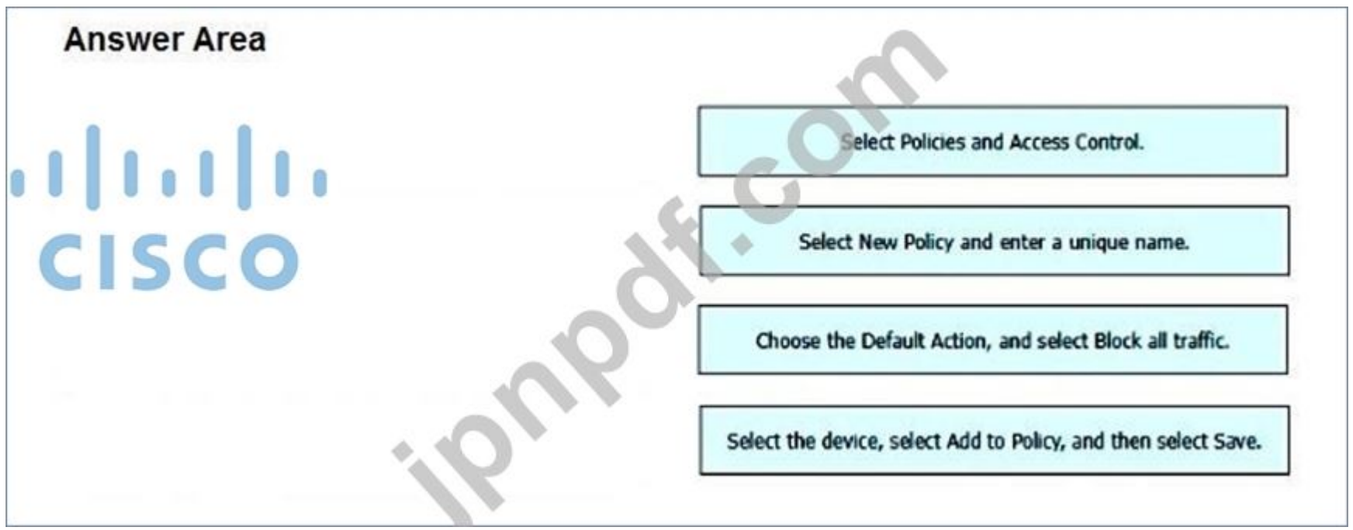
A. アクセス ポリシーによってトラフィックがブロックされています。
B. パケットキャプチャはブロックされたトラフィックのみを表示します
C. FTD には Web サーバへのルートがありません。
D. キャプチャでは、Web サーバーのパブリック IP アドレスを使用する必要があります。
Answer: D (メーッセージを残す)

最新問題: **51**
Cisco FMC が Cisco ISE と統合されている場合、使用できる 2 つの修復オプションはどれですか。
（2つ選択してください。）
A. 動的ヌルルートが設定されました
B. DHCPプールの無効化
C. 隔離
D. ポートのシャットダウン
E. ホストのシャットダウン
Answer: C,D (メーッセージを残す)
Firepower 6.1 修復モジュールにより、相関ルールが一致した場合に、Firepower システムは ISE EPS 機能 (隔離、隔離解除、ポート シャットダウン) を修復として使用できるようになります。
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediati.html

最新問題: **52**
ドラッグアンドドロップの質問
エンジニアは、Cisco Secure Firewall Management Center で基本的なアクセス制御ポリシーを作成し、デフォルトですべてのトラフィックをブロックする必要があります。左側の設定アクションを右側のシーケンスにドラッグ＆ドロップします。



Answer:



Explanation:
この順序は、論理的な FMC ワークフローに従います。ポリシー セクションに移動し、新しいポリシーを作成し、その動作 (デフォルトのアクション) を定義し、最後に適切なデバイスに割り当てます。

最新問題: **53**
エンジニアがCisco Secure Firewall Management Centerを使用してCiscoセキュリティデバイスを設定しています。ローカルシステム上のCA証明書バンドルとCiscoサーバの最新のCAバンドルを比較するには、どの設定コマンドを実行する必要がありますか？
A. cert-update run-now を設定します
B. 証明書更新テストを構成する
C. cert-update compare を設定する
D. cert-update の自動更新を有効にする設定
Answer: (解答を表示する**)**
configure cert-update compare コマンドは、Cisco Secure Firewall Management Center で使用され、ローカル CA 証明書バンドルとシスコのアップデートサーバから入手可能な最新のバンドルを比較します。これにより、手動または自動アップデートを実行する前に、ローカルシステムに最新の CA 証明書があるかどうかを確認できます。

最新問題: **54**
VPN管理者は、Cisco Secure Firewall Management Centerによって管理されているCisco Secure Firewall Threat Defenseインスタンスのリモートアクセス VPN認証をLDAPからLDAPS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. 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
B. LDAPS サーバー証明書をセキュアファイアウォール管理センターのレルムに追加する必要があります
C. セキュアファイアウォール管理センター証明書をLDAPSサーバーに追加する必要があります
D. 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
Answer: B (メーッセージを残す**)**
Windows Server の 「オブジェクト > PKI > 信頼された CA > 信頼された CA の追加」で、LDAPS サービス証明書に署名したルート CA 証明書をインポートします。これは、レルムのディレクトリ サーバー構成で参照されます。
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client- v4x/220880-configure-password-management-using-ldap.html#toc-hId--2065014694

最新問題: **55**
セキュリティ エンジニアが複数のブランチ ロケーションに対してアクセス制御ポリシーを構成しています。
これらの場所は共通のルール セットを共有し、各場所のローカルで重要な内部ネットワーク サブネットを含む INSIDE_NET と呼ばれるネットワーク オブジェクトを利用します。
各場所でポリシーの一貫性を維持しながら、適用可能なルール内でローカルで重要なネットワーク サブネットのみを許可するには、どのような手法がありますか?
A. INSIDE_NETネットワークオブジェクトとオブジェクトオーバーライドを使用してACPを作成する
B. Cisco Talosから更新される動的ACPを利用する
C. デバイスごとに一意のACPを作成する
D. ポリシー継承を利用する
Answer: A (メーッセージを残す**)**

最新問題: **56**
アプリケーション層プリプロセッサにはどのようなものがありますか? (2 つ選択してください。)
A. CIFS
B. IMAP
C. SSL
D. DNP3
E. ICMP
Answer: B,C (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Applic

最新問題: **57**
展示を参照してください。他のすべてのウェブサイトへの同様の通信を防ぎながら、このウェブサイトへのアクセスを修正するには、何をする必要がありますか？

```
    6: 15:46:24.605132 192.168.40.11.65830 > 172.1.1.50.80:
SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale
8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group
HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY:
FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-
location: frame 0x00005587afa07120 flow (NA)/NA
```

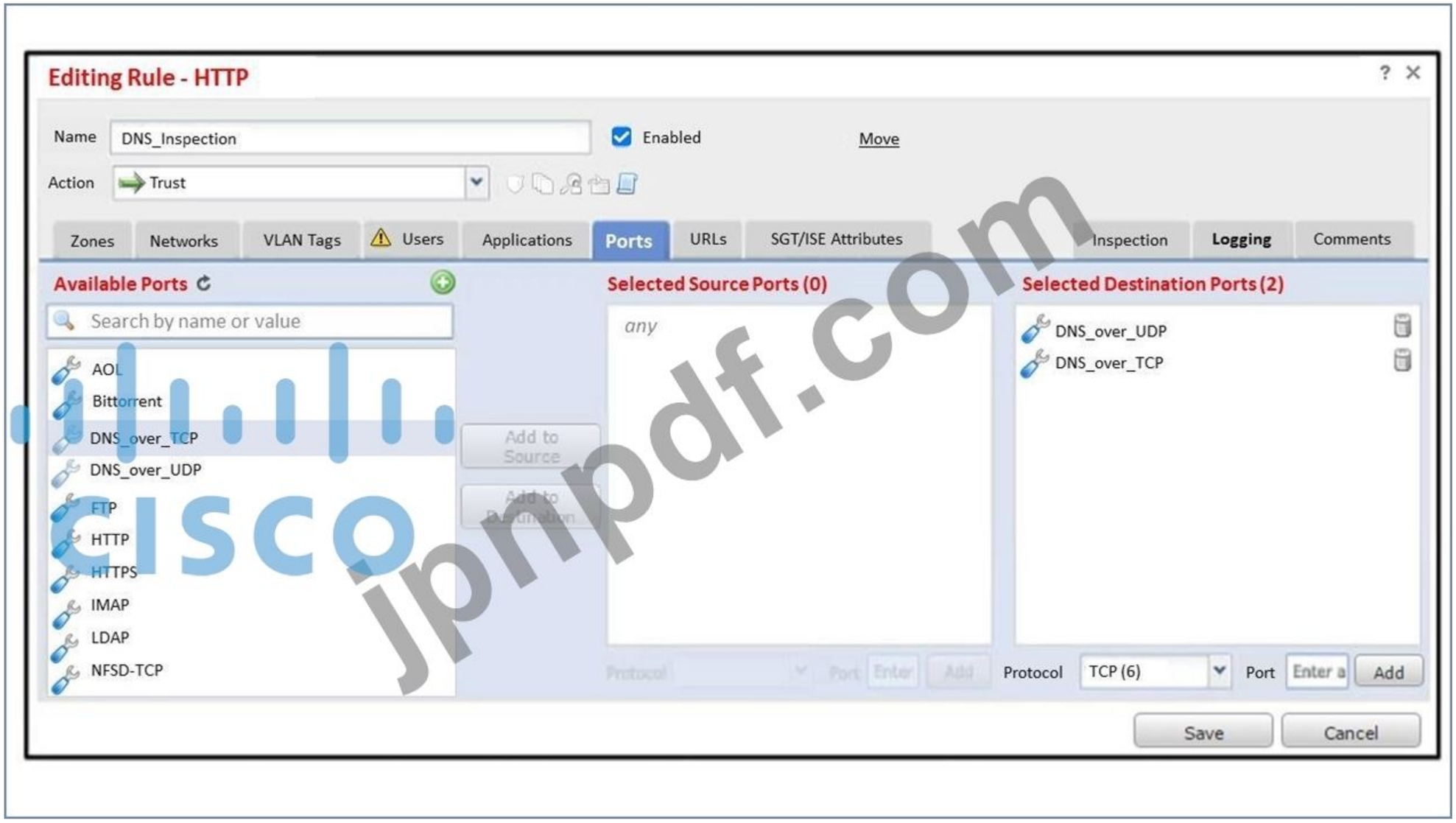
A. ポート 80 を 172.1.1.50 のみに許可するアクセス制御ポリシー ルールを作成します。
B. ポート 443 を 172.1.1.50 のみに許可するアクセス制御ポリシー ルールを作成します。
C. Snort がポート 443 を 172.1.1.50 のみに許可するように侵入ポリシー ルールを作成します。
D. Snort がポート 80 を 172.1.1.50 のみに許可するように侵入ポリシー ルールを作成します。
Answer: A (メーッセージを残す**)**

最新問題: **58**
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. Cisco セキュア ファイアウォール VDC
B. Cisco ISE コンテキスト
C. (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)
D. TACACS+デー タベース
E. AD定義
Answer: (解答を表示する**)**

最新問題: **59**
セキュリティエンジニアは、最近導入したCisco FTDのポリシーを設定する必要があります。会社のセキュリティポリシーでは、2分以内に外部ソースから5件以上の接続が開始された場合、警戒レベルが 高い」とされています。この状況が発生した際にアラートを生成するには、Cisco FMCでどのようなポリシーを設定する必要がありますか？
A. 相関関係
B. アプリケーション検出器
C. 侵入
D. アクセス制御
Answer: (解答を表示する**)**

最新問題: **60**
エンジニアはCisco FMC上で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. 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。
B. オブジェクト内のプロトコルを指定します。
C. CRL 配布ポイントからのすべての URL を含めます。
D. サブジェクト共通名の値を使用します。
Answer: (解答を表示する**)**

最新問題: **61**
図を参照してください。エンジニアがアクセス制御ポーキーを変更し、ファイアウォールを通過するすべてのDNSトラフィックを検査するルールを追加しています。
変更を加えてPokeyを導入した後、DNSトラフィックがSnortエンジンによって適切に検査されないことがわかりました。何が問題なのでしょうか？



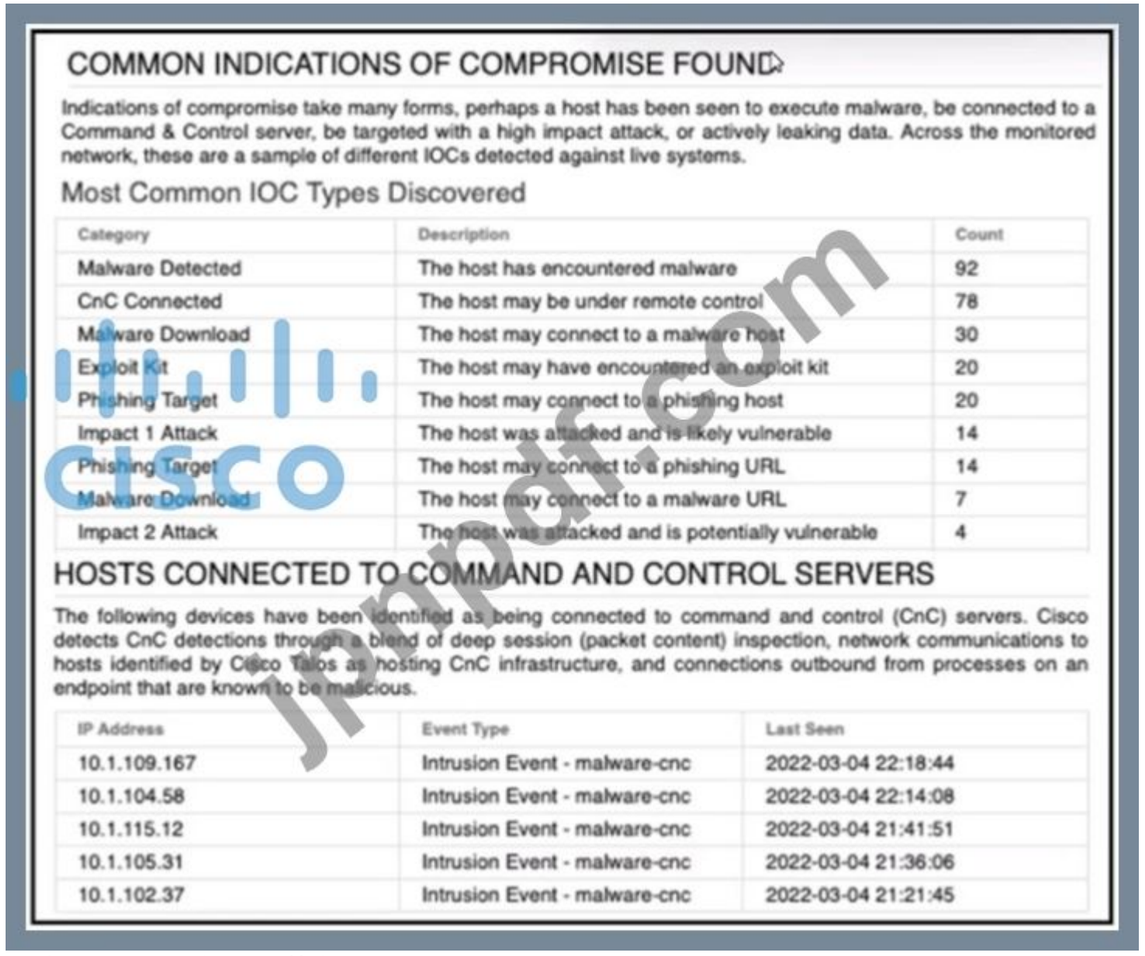
A. ルールのアクションは、許可ではなく信頼に設定されています。
B. ルールはトラフィックの発信元となるセキュリティゾーンを指定する必要があります
C. ルールは検査の送信元ネットワークとポートを定義する必要があります
D. ルールの送信元ポートの設定が間違っています
Answer: (解答を表示する**)**

最新問題: **62**
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. システム生成すべてのトラブルシューティング
D. テクニカルサポートを表示
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

最新問題: **63**
FTD ユニットを IP アドレス 10.0.0.10 にあり、登録キー Cisco123 を持つ FMC マネージャに関連付けるには、FTD ユニットでどのコマンドを実行しますか?
A. マネージャのローカル 10.0.0.10 Cisco123 を設定します
B. マネージャの設定にCisco123 10.0.0.10を追加します
C. マネージャのローカル Cisco123 10.0.0.10 を設定します。
D. マネージャの設定に 10.0.0.10 Cisco123 を追加します
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

最新問題: **64**
エンジニアはCisco FMCの設定で、インターフェースを介したパケット処理の許容時間を制限したいと考えています。しかし、設定時間を超過した場合、パケットが検出をバイパスできるようにする必要があります。
このタスクを実行するには、Cisco FMC で何を設定する必要がありますか?
A. 自動アプリケーションバイパス
B. Cisco ISE セキュリティ グループ タグ
C. ローカルトラフィックバイパスを検査する
D. 高速パスルールバイパス
Answer: A (メーッセージを残す**)**

最新問題: **65**
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ます。リスクを軽減するために、エンジニアはどのような実装を推奨すべきでしょうか？



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

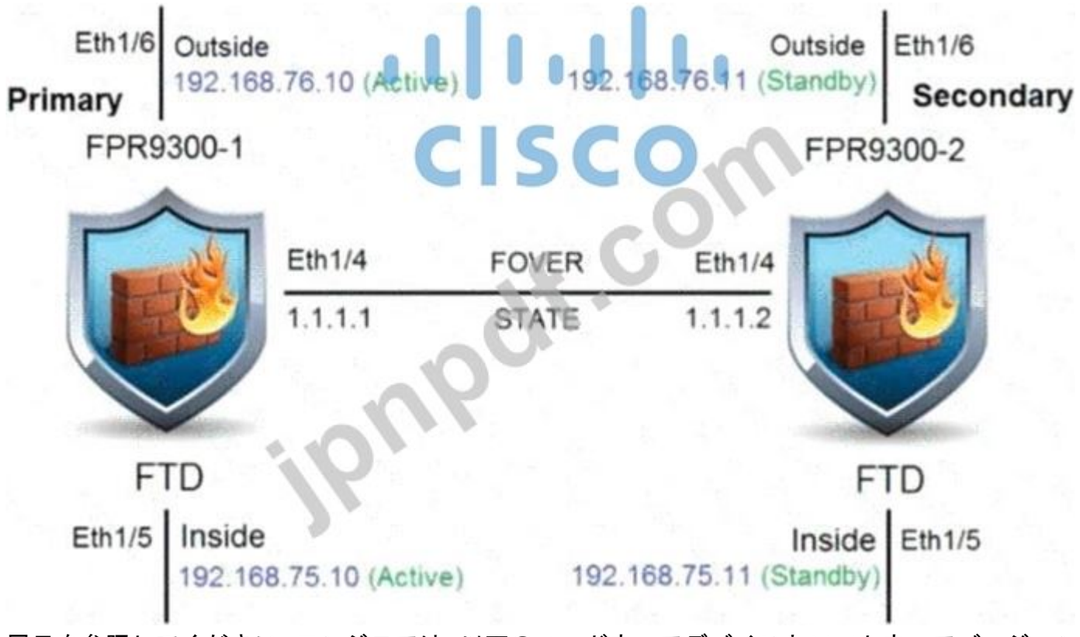
HOSTS CONNECTED TO COMMAND AND CONTROL SERVERS

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

A. ネットワークベースの検出
B. IPアドレスとURLのブラックリスト
C. トレンド分析
D. 仮想保護
Answer: (解答を表示する**)**

最新問題: **66**



展示を参照してください。エンジニアは、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)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ソフトウェア Cisco Secure Firewall Threat Defense 6.0.1.1 (ビルド 1023)
* SW 6.0.1.1 ビルド 1023）を搭載した 1 台の Cisco Secure Firewall Management Center 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. バージョン番号には同じパッチ番号が必要です。
B. 少なくとも 1 つのファイアウォール インターフェイスで DHCP を構成する必要があります。
C. 両方のファイアウォールのインターフェースの数は同じである必要があります。
D. 両方のファイアウォールが透過モードになっている必要があります。
Answer: C (メーッセージを残す**)**

最新問題**: 67**
ある企業では、Cisco FMC によって管理される Cisco FTD を使用した侵入防止を導入中です。
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。このタスクを実現するアクションはどれですか？
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ときに、『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ときに、『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。
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ときに、『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。
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ときに、『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。
Answer: (解答を表示する**)**

最新問題**: 68**
エンジニアはCisco Secure Firewall Threat Defenseインスタンスを導入する必要があります。企業は、Secure Firewall Threat Defenseを導入することで、あらゆる障害発生時でも業務トラフィックを保護したいと考えています。また、データセンターの境界においてIPSに起因する接続障害が発生しないようにする必要があります。エンジニアはどの実装モードを使用する必要がありますか？
A. インラインセット

B. 受動態
C. ハードウェアバイパス
D. Snort フェールオープン
Answer: (解答を表示する**)**

最新問題**: 69**
ある組織では、インラインモードで稼働するCisco IPSを使用して、トラフィックに悪意のあるアクティビティがないか検査しています。Cisco IRSがトラフィックを受信した場合、ドロップされない場合、トラフィックはどのようにして宛先に到達するのでしょうか？
A. Cisco IPS インライン セットから再送信されます。
B. パケットが複製され、そのコピーが宛先に送信されます。
C. Cisco IPS 外部インターフェイスから送信されます。
D. 送信のために Cisco ASA インターフェイスにルーティングされます。
Answer: (解答を表示する**)**
インライン インターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットから再送信されます。
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

最新問題**: 70**
Cisco FirePOWER Threat Defense ソフトウェアでは、トラフィックがアプライアンスを通過するものの VLAN の書き換えを必要としない IPS 展開ではどのインターフェイス モードを設定しますか?
A. インラインセット
B. 受動態
C. インラインタップ
D. ルーティング
E. 透明
Answer: A (メーッセージを残す**)**
インラインセット（バンプオンワイヤモードとも呼ばれます）は、ルーティングやVLANの書き換えを必要とせず、トラフィックがアプライアンスを透過的に通過することを可能にします。トラフィックはインラインでIPS検査を通過するだけです。

最新問題**: 71**
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. システム生成すべてのトラブルシューティング
D. テクニカルサポートを表示
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

最新問題**: 72**
タップ モードでインライン ペア インターフェイスを使用する Cisco Firepower NGIPS 展開の説明のうち、正しいものを 2 つ選択してください。
A. Cisco ASAエンジンのすべての機能が利用可能

B. デプロイメントは透過モードでのみ使用できます。
C. 2 つの物理インターフェースが内部的にブリッジされています。
D. トランジットトラフィックはドロップされる可能性があります
E. 2 つ以上のインターフェースをブリッジできます。
Answer: C,D (メーッセージを残す**)**

最新問題**: 73**
Syslog を使用するのではなく、Cisco Firepower 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直接 Cisco Threat Response にイベントを送信する利点は何ですか?
A. Firepower 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。
B. すべてのタイプの Firepower デバイスがサポートされています。
C. サポートされているバージョンの Firepower を実行しているすべてのデバイスをサポートします。
D. オンプレミスのプロキシサーバーはセットアップやメンテナンスの必要がない
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco
_Threat_Response_Integration_Guide/about_integrating_firepower_and_cisco_threat_response。
html

最新問題**: 74**
ある組織が、マルチコンテキストモードで動作しているCisco ASAデバイスをCisco FTDデバイスに移行しようとしています。Cisco ASA上の各コンテキストがCisco FTDデバイス内で論理的に分離されていることを確認するには、どのような対策を講じる必要がありますか？
A. Cisco FTD デバイスを Cisco ASA ポート チャネルに追加します。
B. Cisco ASA の各コンテキストに対して、Cisco FTD でコンテナ インスタンスを設定します。
C. 各 Cisco FTD コンテキストにトラフィックを分散するためのネイティブ インスタンスを追加します。
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 Cisco FTD を設定します。
Answer: A (メーッセージを残す**)**

最新問題**: 75**
Cisco Threat Response におけるケースブック機能の役割は何ですか?
A. 脅威アナリストの共有
B. ブラウザ拡張機能経由でデータを取得する
C. アラート機能付きトリアージオートマトン
D. アラートの優先順位付け
Answer: A (メーッセージを残す**)**
ケースブックとピボットメニューは、Cisco Threat Responseで利用可能なウィジェットです。ケースブックは、主に調査と脅威分析中に、関心のある観測対象セットを記録、整理、共有するために使用されます。ケースブックを使用すると、観測対象に関する最新の判定や処置状況を取得できます。
https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

最新問題**: 76**

展示を参照してください。エンジニアは、アクセス制御ポーキーを変更して、ファイアウォールを通過するすべての DNS トラフィックを検査するルールを追加しています。変更を加えてポーキーを展開した後、DNS トラフィックが Snort エンジンによって完全に検査されていないことがわかりました。問題は何でしょうか。

A. ルールの送信元ポートの設定が間違っています

B. ルールはトラフィックの発信元となるセキュリティゾーンを指定する必要があります

C. ルールは検査の対象となる送信元ネットワークとポートを定義する必要があります

D. ルールのアクションは、許可ではなく信頼に設定されています。

Answer: D (メーッセージを残す)

最新問題: **77**

エンジニアは、Cisco Secure Firewall Management Center を使用している各部門のネットワークへの ICMP トラフィックを拒否する必要があります。エンジニアは、各ネットワークの関連デバイスで同じオブジェクトを使用する必要があります。Secure Firewall Management Center ではどのような設定が必要ですか？

A. オーバーライドを許可するチェックボックス

B. IPアドレス

C. ICMPを拒否するチェックボックス

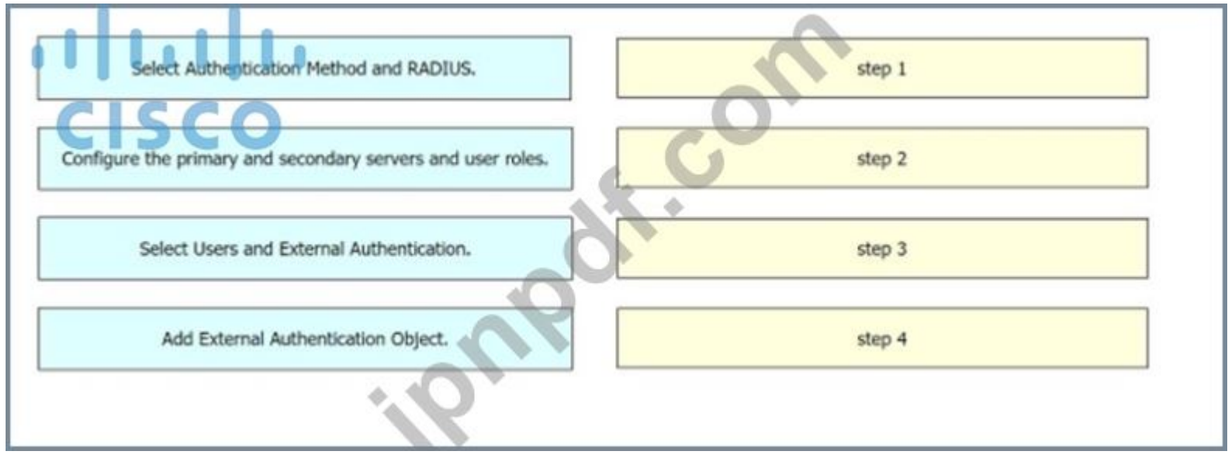
D. IP範囲

Answer: A (メーッセージを残す)

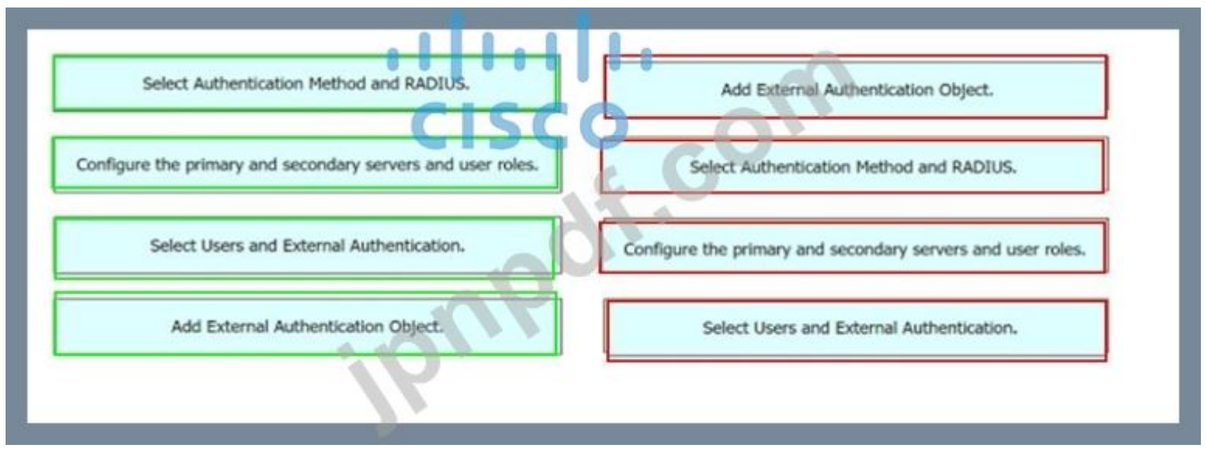
Cisco Secure Firewall Management Center（FMC）では、エンジニアが複数のデバイスまたはネットワークに同じオブジェクトを適用する必要があるものの、デバイスまたはネットワークごとに個別の設定を行いたい場合、「オーバーライドを許可」オプションを使用できます。「オーバーライドを許可」チェックボックスをオンにすると、オブジェクトを一元管理しながら、デバイスごとに異なる設定や値を適用できるため、柔軟性が向上します。これは、単一のオブジェクトを複数のネットワークに適用する場合に便利です。これにより、エンジニアはオブジェクト管理の一貫性を維持しながら、各部門の設定をカスタマイズできます。

最新問題: **78**
管理者は、NAT ID が NAT001、パスワードが Cisco0420l06525 である 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。FMC サーバのプライベート IP アドレスは 192.168.45.45 です。
これはパブリックIPアドレス209.165.200.225/27に変換されます。このタスクを実行するには、どのコマンドセットを使用する必要がありますか？
A. マネージャーを設定して 209.165.200.225/27 <reg_key> <nat_id> を追加します
B. マネージャーを設定して 192.168.45,45 <reg_key> <nat_id> を追加します
C. 設定マネージャーに 209.165.200.225 <reg_key> <nat_id> を追加します
D. マネージャーの設定に 209.165.200.225 255.255.255.224 <reg_key> <nat_id> を追加します
Answer: C (メーッセージを残す**)**

最新問題: **79**
左側の設定手順を右側のシーケンスにドラッグ アンド ドロップして、Cisco FMC で RADIUS サーバーへの外部認証を有効にします。



Answer:



最新問題: **80**
エンジニアがCisco Secure Firewall Threat Defenseデバイスを設定している際に、新たなゼロデイエクスプロイトのデータペイロードに特定のパターンが検出されたため、新しい侵入ルールを作成するように警告されました。ルールの作成者と作成日を識別する行を追加するには、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. コンテンツ
C. 参照
D. gtp_info
Answer: (解答を表示する**)**
Cisco Secure Firewall Threat Defense (FTD) デバイスで新しい侵入ルールを作成する場合は、キーワード タイプ 「metadata」を使用して、ルールの作成者と作成日を識別する行を追加する必要があります。
メタデータ キーワードは、作成者や作成日など、ルールに関する追加情報を保存するために使用されます。
手順:
* FMC で、[ポリシー] > [侵入] > [ルール] に移動します。
* 新しいルールを作成するか、既存のルールを編集します。
* 「metadata」キーワードを使用して、作成者と日付に関する情報を追加します。
例：
メタデータ: created_at 2023-06-15、作成者 「John Doe」;
メタデータ キーワードを使用すると、ルールの作成と作成者を追跡するための関連情報がルールに含まれることが保証されます。これは、ルールのドキュメントと説明責任を維持するために不可欠です。
参考資料:Cisco Secure Firewall Management Center 侵入ポリシー ガイド、カスタム ルールの作成とメタデータの使用に関する章。

最新問題: **81**
Cisco Threat Response におけるケースブック機能の役割は何ですか?
A. 脅威アナリストの共有
B. ブラウザ拡張機能経由でデータを取得する
C. アラート機能付きトリアージオートマトン
D. アラートの優先順位付け
Answer: A (メーッセージを残す**)**
説明
ケースブックとピボットメニューは、Cisco Threat Responseで利用可能なウィジェットです。ケースブックは、主に調査と脅威分析中に、関心のある観測対象セットを記録、整理、共有するために使用されます。
ケースブックを使用すると、観測対象に関する最新の判定や処置状況を取得できます。
https://www.cisco.com/c/en/us/td/docs/se
curity/ces/ユーザーガイド/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces
_13-5-1/b_ESA_管理ガイド_13-0_chapter_0110001.pdf

最新問題: **82**
Cisco Secure Firewall Threat Defenseデバイスは、インラインIPSモードで設定されており、インラインセット内のインターフェー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ることなく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設定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. 厳密なTCP強制

D. タップモード
Answer: B (メーッセージを残す**)**
インラインIPSモードでは、VDB（脆弱性データベース）アップデートの適用中にトラフィックが中断されることなく通過できるようにするため、「Short Fall Open」設定が必要です。この設定により、アップデート中や検査エンジンの障害など、検査プロセスに問題が発生した場合でも、トラフィックはファイアウォールを通過できます。
手順:
* FMC で、インライン セット設定に移動します。
* 「Short Fall Open」オプションを有効にします。
* 設定を FTD デバイスに展開します。
これにより、更新中や検査プロセスでのその他の問題の発生時にネットワーク トラフィックが中断されることがなくなります。
参考資料: Cisco Secure Firewall Threat Defense 構成ガイド、インライン IPS モード構成の章。

最新問題**: 83**
ネットワークエンジニアは、Cisco Secure Firewall Threat DefenseデバイスにIPSモードを設定してトラフィックを検査し、IDSとして機能するようにする必要があります。エンジニアは既に、セキュアファイアウォール Threat Defenseデバイスのパッシブインターフェースとスイッチの SPANを設定しています。次にエンジニアは何を設定する必要がありますか？
A. セキュアファイアウォール脅威防御デバイスの侵入ポリシー
B. セキュアファイアウォール脅威防御デバイスのアクティブインターフェース
C. スイッチ上のDHCP
D. スイッチ上のアクティブなSPANポート
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスでIPSモードを設定し、トラフィックを検査してIDSとして動作させるには、ネットワークエンジニアがFTDデバイスに侵入ポリシーを設定する必要があります。スイッチのパッシブインターフェイスとSPANはすでに設定されており、トラフィックはFTDにミラーリングされています。次のステップは、悪意のあるトラフィックを検出して対応するためのルールとアクションを定義する侵入ポリシーを設定することです。
手順:
* FMC で、[ポリシー] > [侵入] に移動します。
* 新しい侵入ポリシーを作成するか、既存の侵入ポリシーを編集します。
* 脅威を検出するためのルールとアクションを定義します。
* 侵入ポリシーを関連するインターフェースまたはアクセス制御ポリシーに適用します。
この設定により、FTD はミラーリングされたトラフィックを検査し、定義された侵入ポリシーに基づいて適切なアクションを実行できるようになります。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、侵入ポリシーの章。

最新問題**: 84**
エンジニアが、Secure Firewall Management Center 7.0 GUIを使用して、Cisco Secure Firewall Threat Defenseデバイスのアップグレードに関するトラブルシューティングを行っています。エンジニアはアップグレードデータとログを収集したいと考えています。エンジニアが実行する必要がある2つのアクションはどれですか？ （2つ選択してください。）
A. システムとトラブルシューティングの詳細を表示します。
B. Secure Firewall Threat Defense デバイスのプロパティを選択します。
C. セキュア ファイアウォール管理センター デバイスを選択します。
D. ヘルス イベント ページにアクセスします。
E. ヘルス モニター ページにアクセスします。
Answer: A,E (メーッセージを残す**)**

FMC で、[Health] > [Monitor] に移動し、FTD デバイスを選択して、システムとトラブルシューティングの詳細を開き、アップグレード ログとデータ バンドルをダウンロードします。

最新問題: **85**
ネットワーク管理者は、Cisco Secure Firewall Threat Defenseを2つのISPとBGP経由でピアリングするように設定しようとしています。管理者は、特定のIPアドレス範囲へのトラフィックが、一方のISPではなくもう一方のISPに優先的に到達するようにしたいと考えています。この要件を満たすには、ピアへのBGP接続でどのような設定を行う必要がありますか？
A. プレフィックスリスト
B. アクセスリスト
C. アドレスマップ
D. ルートマップ
Answer: D (メーッセージを残す**)**
ルートマップは、BGPルーティングの優先度を制御するための適切なメカニズムです。管理者は、重み、ローカル優先度、ASパスなどの属性を変更することで、ルート選択に影響を与えるポリシーを定義できます。特定のIPアドレス範囲へのトラフィックが特定のISPを他のISPよりも優先するようにするには、管理者はルートマップを設定して、それらのルートのBGP属性を操作し、目的のISPのローカル優先度を上げるなどすることができます。

最新問題: **86**
管理者がCisco FTDの導入環境にQoSポリシーを追加しようとしています。ポリシーに新しいルールを追加し、 宛先インターフェイスオブジェクトのインターフェイス」にQoSを適用すると、インターフェイスオブジェクトが利用できなくなります。何が問題なのでしょうか？
A. QoS はルーティングされたインターフェイスでのみ使用可能であり、このデバイスは透過モードです。
B. インターフェースが存在するネットワークセグメントに連続したIP空間がありません
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. 宛先インターフェースタイプ間に競合があり、QoS を追加できません。
Answer: A (メーッセージを残す**)**

最新問題: **87**
ネットワーク管理者は、高可用性を実現するために、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。管理者はどこにEtherChannelインターフェイスを作成する必要がありますか？
A. FMC CLI
B. FTD CLI
C. FXOS CLI
D. FMC GUI
Answer: (解答を表示する**)**
説明
EtherChannelインターフェースは、単一のネットワークリンクとして機能する個々のイーサネットリンクのバンドルで構成される論理インターフェースです。EtherChannelインターフェースは、ネットワーク接続の帯域幅と信頼性を向上させることができます5。
高可用性のためにFMCに登録されたCisco Firepower 9300アプライアンスでは、ネットワーク管理者がFXOS CLIでEtherChannelインターフェイスを作成する必要があります。FXOSは、Firepower 9300シャーシ上で動作するオペレーティングシステムであり、インターフェイス設定、電源ステータス、ファン速度制御などのハードウェア管理機能を提供します6。
FXOS CLI で EtherChannel インターフェイスを作成するには、ネットワーク管理者は次の手順に従います5。
SSH またはコンソールを使用して FXOS CLI に接続します。
イーサネット アップリンク モードに入るには、scope eth-uplink コマンドを入力します。
EtherChannel インターフェイスを作成するには、create port-channel コマンドを入力します。

EtherChannel インターフェイスのポートチャネル ID (1 ～ 48) とモード (オンまたはアクティブ) を入力します。
EtherChannel インターフェイスに物理インターフェイスを追加するには、add interface コマンドを入力します。
物理インターフェースの 1 つ以上のインターフェース ID (たとえば、1/1) を入力します。
変更を保存するには、commit-buffer コマンドを入力します。
その他のオプションは、次の理由により正しくありません。
FMC CLIには、Firepower 9300アプライアンスにEtherChannelインターフェイスを作成するためのコマンドは用意されていません。FMC CLIは主に、バックアップ、復元、アップグレード、トラブルシューティングなどのFMC設定の管理に使用されます7。
FTD CLI には、Firepower 9300 アプライアンス上で EtherChannel インターフェイスを作成するためのコマンドは用意されていません。FTD CLI は主に、ルーティング、NAT、VPN、アクセス制御などの FTD 設定の管理に使用されます8。
FMC GUIには、Firepower 9300アプライアンスにEtherChannelインターフェイスを作成するためのオプションはありません。FMC GUIは主に、アクセス制御、侵入検知、ファイル、マルウェア対策などのFTDポリシーの管理に使用されます9。

最新問題: **88**
しきい値設定はどの 2 つの場所で設定できますか? (2 つ選択してください。)
A. 各IPSルール
B. ネットワーク分析ポリシー内でグローバルに
C. 侵入ポリシーごとにグローバルに
D. 各アクセス制御ルール
E. プリプロセッサごとに、ネットワーク分析ポリシー内
Answer: A,C (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.pdf

最新問題: **89**
エンジニアは、Cisco Secure Firewall 上の既存のカスタム サーバ フィンガープリントをレビューしています。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アクションを実行する必要がありますか。
A. ネットワークセグメントのNetFlow監視を追加する
B. スキップする必要があるポートを除外します。
C. マルチドメイン環境内の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。
Answer: (解答を表示する**)**
Cisco Secure Firewall におけるカスタム サーバ フィンガープリントの精度を向上させるには、誤検知につながる可能性のあるポートや、ホスト上の実際のサービスを代表しないポートを除外する必要があります。これにより、システムは関連トラフィックのみに集中できるようになり、より正確なネットワーク検出とフィンガープリントが可能になります。

最新問題: **90**
ある組織では、Cisco FTDとCisco ISEを使用してアイデンティティベースのアクセス制御を行っています。ネットワーク管理者がCisco FTDのイベントを分析したところ、未知のユーザートラフィックがファイアウォールを通過できていることに気付きました。正当なユーザートラフィックを許可しながら、このトラフィックをブロックするには、どのように対処すればよいでしょうか？
A. Cisco ISE 許可ポリシーを変更して、ユーザへのこのアクセスを拒否します。
B. 正当なユーザー名のみを Cisco FTD に送信するように Cisco ISE を変更します。
C. Cisco FTD のアクセス コントロール ポリシーに不明なユーザーを追加します。

D. Cisco FTD のマルウェアおよびファイル ポリシーに不明なユーザーを追加します。
Answer: C (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-identity

最新問題**: 91**
ネットワークエンジニアは、Cisco Secure Firewall Management Center と Cisco Secure Firewall Threat Defense 間の接続に問題があることを検出しました。初期トラブルシューティングの結果、ハートビートとイベントが受信されていないことが判明しました。エンジニアは両ピア間のセキュアチャネルを再確立しました。この問題を解決するために、エンジニアが実行する必要があるコマンドはどれですか？ 2つ選択してください。）
A. manage_procs.pl
B. ディスクマネージャーを表示
C. 履歴を表示
D. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
E. sudo stats_unified.pl
Answer: A,E (メーッセージを残す**)**
Cisco Secure Firewall Management Center (FMC) と Cisco Secure Firewall Threat Defense (FTD) デバイス間で接続の問題が検出され、初期トラブルシューティングでハートビートとイベントが受信されていないことが判明した場合、エンジニアは次のコマンドを実行して、安全なチャネルを再確立し、プロセス ステータスをチェックすることで問題を解決できます。
manage_procs.pl: このスクリプトは、FTD デバイス上のプロセスを管理および再起動するために使用されます。
このスクリプトを実行すると、誤動作しているプロセスを再起動し、FMC と FTD 間の接続を再確立するのに役立ちます。
sudo stats_unified.pl: このコマンドは、統合システムプロセスの詳細な統計情報とステータスを提供します。セキュアチャネルとイベントレポートに関連する問題の診断と解決に役立ちます。
手順:
FTD CLI にアクセスします。
プロセスを再起動したい場合は、manage_procs.pl コマンドを実行します。
詳細なプロセス統計を収集し、ステータスを確認するには、コマンド sudo stats_unified.pl を実行します。
これらのコマンドは、必要なすべてのプロセスが正しく実行され、安全なチャネルが再確立されていることを確認することで、接続の問題を解決するのに役立ちます。

最新問題**: 92**
エンジニアは、トラフィックのホップ数を増やすことなく、単一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設定する必要があります。エンジニアはどのようにこれを実現するでしょうか？
A. Cisco Firepower を FXOS モニタ専用モードで設定します。
B. Cisco Firepower を透過型ファイアウォールとして設定する
C. Cisco Firepower を Cisco FDM で管理されるように設定します
D. Cisco Firepowerを侵入防止モードで設定する
Answer: (解答を表示する**)**

最新問題: **93**
ネットワーク管理者は、Cisco FTDの背後にあるルータへのサイト間IPsec VPNを設定しています。管理者は、このデバイスへのUDPトラフィックを許可するアクセスポリシーを設定しています。500、4500、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には、どのような操作が必要ですか？
A. アクセス ポリシーで IPsec 検査を有効にします。
B. アクセス ポリシーを変更して、すべてのポートを許可します。
C. 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。
D. 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。
Answer: A (メーッセージを残す**)**

最新問題: **94**
パケットキャプチャにトレース オプションを選択する利点は何ですか?
A. このオプションは、パケットがドロップされたか成功したかを示します。
B. 宛先ホストが別のパスを介して応答するかどうかを示すオプション。
C. このオプションは、キャプチャされるパケットの数を制限します。
D. このオプションは各パケットの詳細をキャプチャします。
Answer: C (メーッセージを残す**)**
セクション: 管理とトラブルシューティング
説明/参照:

最新問題: **95**
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. coredump packet-engine 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
Answer: C (メーッセージを残す**)**
理由 :SNORTエンジンのキャプチャには「capture-traffic」コマンドが使用されます。LINAエンジンのキャプチャをキャプチャするには、「capture」コマンドを使用します。LINAエンジンはデバイスの実際の物理インターフェースを表すため、「capture」が唯一の合理的な選択肢です。参考 :https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10 コマンドは、firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 です。firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14 です。

最新問題: **96**
図を参照してください。Cisco Secure Firewall Threat Defense（FTD）デバイスが、インラインセットを使用してインラインモードで導入されています。ネットワークエンジニアは、ルーティング先のルータR1とセキュアFTDデバイス間のケーブルが切断された場合、ルータR2が直接接続されているルート192.168.1.0/24をルーティングテーブルから削除するようにしたいと考えています。エンジニアはどのようなアクションを実行する必要がありますか？

A. Secure FTDデバイスにリンクの古さを伝播するオプションを実装する
B. R1 と R2 の間にルーティング プロトコルを確立します。
C. Secure FTD デバイス上のハードウェア バイパスを無効にします。
D. R2のGi0/2インターフェースに自動ステート機能を実装する
Answer: A (メーッセージを残す**)**
ルータR1とSecure FTDデバイス間のケーブルが切断された際に、ルータR2が192.168.1.0/24への直接接続ルートをルーティングテーブルから削除するようにするには、ネットワークエンジニアがSecure FTDデバイスに 『リンク状態を伝播』オプションを実装する必要があります。このオプションにより、FTDはリンク状態の変化を隣接デバイスに伝播し、切断が認識され、それに応じてルーティングテーブルが更新されます。
手順:
FMC 経由で FTD デバイス構成にアクセスします。
関連するインターフェースのインターフェース設定に移動します。
R1 および R2 に接続されているインターフェースに対して 『リンク状態の伝播』オプションを有効にします。
変更を FTD デバイスに展開します。
この設定により、リンク状態の変更がルータ R2 に伝達され、切断されたルートをルーティング テーブルから削除するように要求されます。

最新問題: **97**
FTD ユニットにログインしたときに、ユニットがローカルで管理されているか、リモート FMC サーバーによって管理されているかを判断するために CLI で実行されるコマンドはどれですか。
A. システム生成トラブルシューティング
B. 設定セッションを表示
C. マネージャーを表示
D. 実行中の設定を表示 | マネージャを含める
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/c_3.html

最新問題: **98**
エンジニアは、Cisco FTD アプライアンスを IPS 専用モードで設定しており、Fail-to-Wire インターフェイスを利用する必要があります。
これらの要件を満たすにはどのインターフェース モードを使用する必要がありますか?
A. 透明
B. ルーティング
C. 受動態
D. インラインセット
Answer: D (メーッセージを残す**)**
参照：

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline

最新問題: **99**
エンジニアがセキュリティゾーンにファイルポリシー設定を展開するアクセス制御ルールを設定したところ、デバイスが再起動しました。再起動の理由は何ですか？
A. ルール内のソース トンネル ゾーンが、宛先ポリシー内のトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
B. アクセス制御ルール内の送信元または宛先のセキュリティ ゾーンは、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致します。
C. ルール内のソース トンネル ゾーンが、ソース ポリシー内のトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
D. ソース トンネル ゾーン内のソースまたは宛先セキュリティ ゾーンが、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致しません。
Answer: (解答を表示する**)**

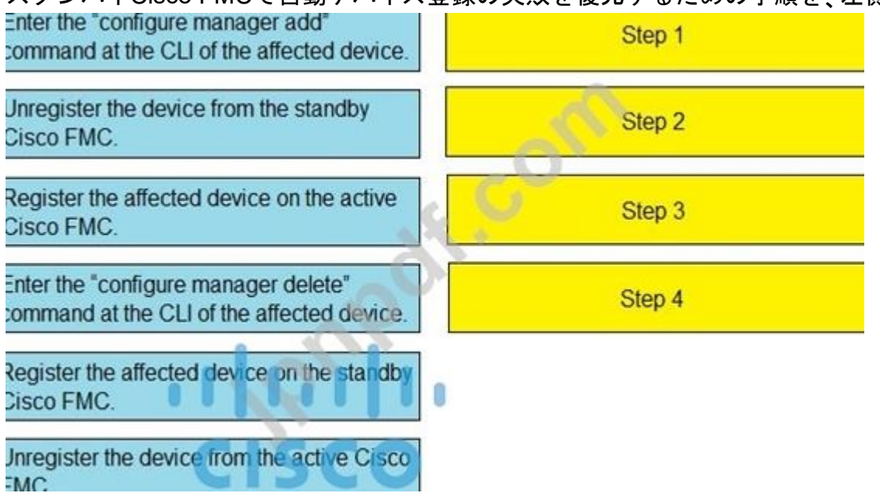
最新問題: **100**
Cisco Secure Firewall Threat Defense（FTD）デバイスでVPNに接続しようとすると、Cisco Duo 2FAが失敗するという報告がユーザーから寄せられています。ITスタッフは多要素認証を必要としないVPNプロファイルを使用しており、問題なくVPNに接続できます。ネットワーク管理者がCisco Secure Firewall Management Centre（FMC）でVPNトラブルシューティングログを確認すると、Cisco Duo AAAサーバーに「テールとしてマークされています」というエラーが表示されています。この問題の根本原因は何ですか？
A. 多要素認証は、Secure FMC 管理対象デバイスではサポートされていません。
B. Secure FTD デバイスに Duo 信頼証明書がありません。
C. Secure FTD デバイスから内部 AD サーバーにアクセスできません。
D. Secure FTD デバイスに AD Trust 証明書がありません。
Answer: B (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスでVPN接続を試みている際にCisco Duo 2FAが失敗するという報告があり、FMCのVPNトラブルシューティングログにCisco Duo AAAサーバが失敗としてマークされていることを示すエラーが表示される場合、根本原因はFTDデバイスにDuo信頼証明書がないことであると考えられます。信頼証明書は、FTDとDuo認証サービス間の安全で信頼できる接続を確立するために不可欠です。
手順:
* 必要な Duo 信頼証明書を取得します。
* FTD デバイスに証明書をインストールします。
* 設定を確認して、FTD デバイスが Duo AAA サーバと適切に通信できることを確認します。
これにより、FTD デバイスが Duo サーバーを信頼できるようになり、認証失敗が解決されます。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、証明書管理の章。

最新問題: **101**
ある組織は、ネットワークにトランスペアレントモードを使用してCisco FTDを導入しています。デフォルトのアクセス制御ポリシーのどのルールが、この導入によってネットワークにループが発生しないことを保証しますか？
A. ARP 検査はデフォルトで有効になっています。
B. マルチキャスト パケットとブロードキャスト パケットはデフォルトで拒否されます。
C. STP BPDU パケットはデフォルトで許可されます。
D. ARP パケットはデフォルトで許可されます。
Answer: C (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

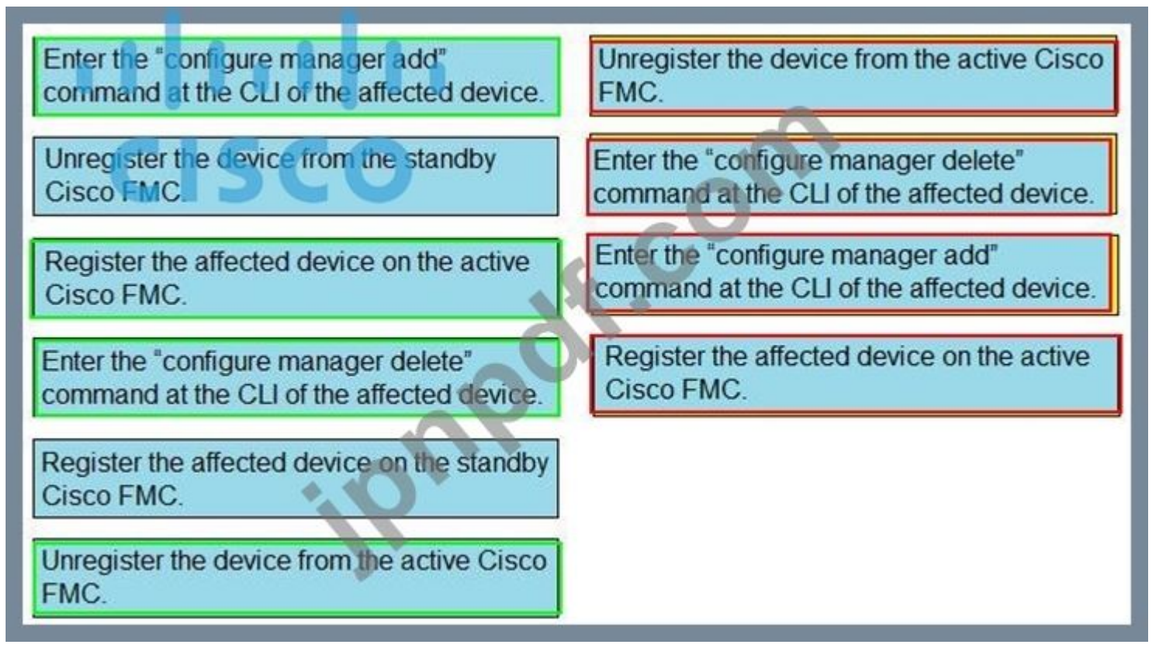
最新問題: **102**
パケット キャプチャによるトラブルシューティング中に、ファイル サイズ コマンド オプションが必要になるのはいつですか?
A. キャプチャパケットが16 MB未満の場合
B. キャプチャパケットが二次メモリから制限されている場合
C. キャプチャパケットが10 GBを超える場合
D. キャプチャパケットが32 MBを超える場合
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

最新問題: **103**
Threat Intelligence Director がサポートするフィルタリングの最大 SHA レベルは何ですか?
A. SHA-256
B. SHA-1024
C. SHA-4096
D. SHA-512
Answer: A (メーッセージを残す**)**

最新問題: **104**
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。

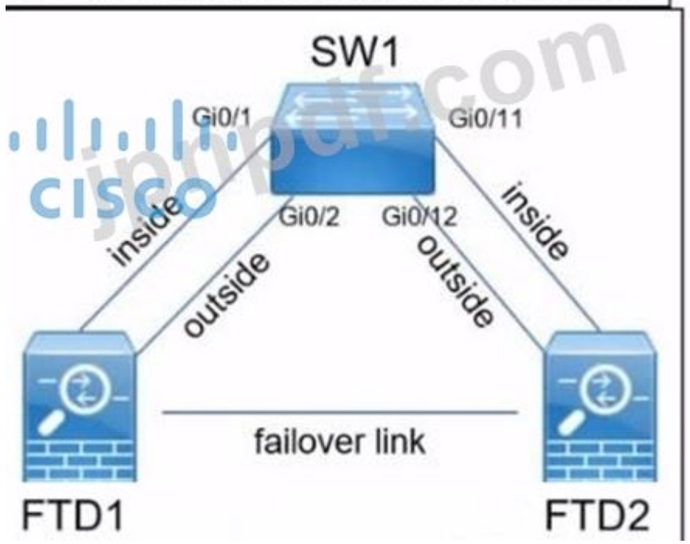


説明
Answer:



最新問題: **105**
展示品を参照してください。

```
Gi0/1 and Gi0/11 configuration:
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown

Gi0/2 and Gi0/12 configuration:
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
```



ある企業では、FTD1 と FTD2 という名前の Cisco Secure Firewall 脅威防御デバイスのペアを導入しています。
FTD1 と FTD2 は、フェールオーバー リンクがあり、ステートフル リンクがないアクティブ/スタンバイ ペアとして設定されています。
FTD1 に障害が発生した場合でも、内部ネットワーク上のユーザーが外部デバイスと通信できるようにするには、次に何を実装する必要がありますか?
A. FTD1 および FTD2 に接続されたスイッチ インターフェイスのポート セキュリティを無効にします。
B. FTD1 および FTD2 のスイッチ インターフェイスで、最大保護アドレスを 2 に設定します。
C. ステートフル リンクを接続して構成し、変更をデプロイします。
D. SW1とFTD2のスパニングツリーPortFasI機能を設定します。
Answer: C (メーッセージを残す)
Cisco Secure Firewall Threat Defense（FTD）デバイスを使用したフェイルオーバー構成では、プライマリデバイス（FTD1）に障害が発生した場合でも、内部ネットワーク上のユーザが外部デバイスとの通信を継続できるようにするため、ステートフルフェイルオーバーリンクを実装する必要があります。ステートフルフェイルオーバーリンクにより、セカンダリデバイス（FTD2）はセッション情報と状態データを維持できるため、シームレスなフェイルオーバーが実現し、中断を最小限に抑えることができます。
ステートフル フェイルオーバー リンクを実装する手順:
* FTD1 と FTD2 の間にステートフル フェールオーバー リンクを物理的に接続します。
* FMC でステートフル フェールオーバー リンクを設定します。
* 両方のデバイスが適切に同期され、ステートフル フェイルオーバーが有効になっていることを確認します。
* 変更を両方の FTD デバイスに展開します。
ステートフル リンクを設定すると、セカンダリ FTD は、ユーザーが接続を再確立する必要なくアクティブなセッションを引き継ぐことができるため、継続的な通信が保証されます。

参考資料: Cisco Secure Firewall Threat Defense 構成ガイド、フェールオーバー構成の章。

最新問題: **106**
ネットワーク管理者は、アクティブ/パッシブ HA Cisco FTD ペアを構成するときに、フェールオーバーに使用するリンクを選択できません。
高可用性ペアを設定する前にどの構成を変更する必要がありますか?
A. 各 Cisco FTD のインターフェイスからインターフェイス名を削除する必要があります。
B. 名前 Failover は、各 Cisco FTD のインターフェイスで手動で設定する必要があります。
C. インターフェイス上の各 Cisco FTD に、同じサブネット内の IP アドレスを追加する必要があります。
D. インターフェイスは、LACP Active/Active EtherChannel の一部として設定する必要があります。
Answer: C (メーッセージを残す**)**

最新問題: **107**

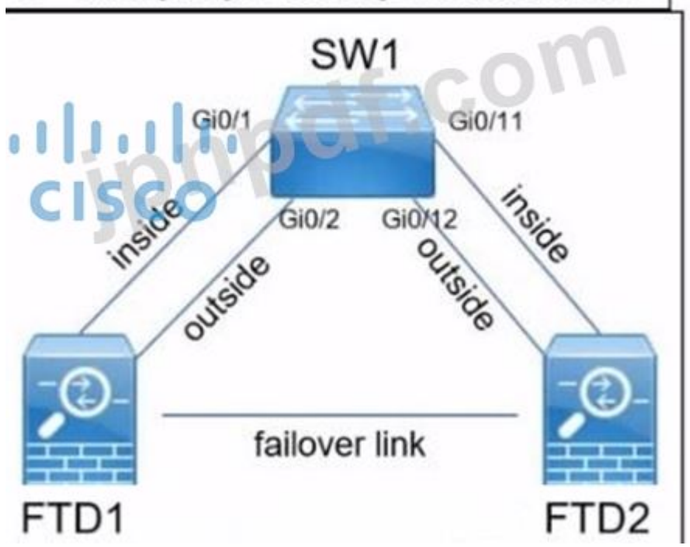
展示を参照してください。エンジニアはアクセス制御ポーキーを変更して、ファイアウォールを通過するすべての DNS トラフィックを検査するルールを追加しています。変更を加えてポーキーを展開した後、DNS トラフィックが Snort エンジンによって完全に検査されていないことがわかりました。問題は何でしょうか。
A. ルールは検査の送信元ネットワークとポートを定義する必要があります

B. ルールはトラフィックの発信元となるセキュリティゾーンを指定する必要があります
C. ルールのアクションは、許可ではなく信頼に設定されています。
D. ルールの送信元ポートの設定が間違っています
Answer: C (メーッセージを残す**)**

最新問題: **108**
Cisco Secure Firewall Threat Defense アプライアンスで複数のブリッジ グループが透過モードで設定されている場合、どの通信がブリッジ グループからブロックされますか?
A. 他のルータと
B. クライアントデバイスと
C. お互いに
D. インターネットで
Answer: C (メーッセージを残す**)**
トランスペアレントモードで動作するCisco Secure Firewall Threat Defenseアプライアンスでは、複数のブリッジグループが互いに分離されています。ブリッジグループ間のトラフィックはデフォルトでブロックされ、明示的にルーティングまたは追加設定によって許可されない限り、通信は同じブリッジグループ内でのみ許可されます。

最新問題: **109**
展示品を参照してください。

```
Gi0/1 and Gi0/11 configuration:
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown

Gi0/2 and Gi0/12 configuration:
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
```



ある企業では、FTD1 と FTD2 という名前の Cisco Secure Firewall 脅威防御デバイスのペアを導入しています。

FTD1とFTD2は、フェイルオーバーリンクはあるものの、ステートフルリンクは備えていないアクティブ/スタンバイペアとして設定されています。FTD1に障害が発生した場合でも、内部ネットワーク上のユーザーが外部デバイスと通信できるようにするには、次に何を実装する必要がありますか？
A. FTD1 および FTD2 に接続されたスイッチ インターフェイスのポート セキュリティを無効にします。
B. FTD1 および FTD2 のスイッチ インターフェイスで、最大保護アドレスを 2 に設定します。
C. ステートフル リンクを接続して構成し、変更をデプロイします。
D. SW1とFTD2のスパニングツリーPortFasI機能を設定します。
Answer: C (メーッセージを残す)
Cisco Secure Firewall Threat Defense（FTD）デバイスを使用したフェイルオーバー構成では、プライマリデバイス（FTD1）に障害が発生した場合でも、内部ネットワーク上のユーザが外部デバイスとの通信を継続できるようにするため、ステートフルフェイルオーバーリンクを実装する必要があります。ステートフルフェイルオーバーリンクにより、セカンダリデバイス（FTD2）はセッション情報と状態データを維持できるため、シームレスなフェイルオーバーが実現し、中断を最小限に抑えることができます。
ステートフル フェイルオーバー リンクを実装する手順:
* FTD1 と FTD2 の間にステートフル フェールオーバー リンクを物理的に接続します。
* FMC でステートフル フェールオーバー リンクを設定します。
* 両方のデバイスが適切に同期され、ステートフル フェイルオーバーが有効になっていることを確認します。
* 変更を両方の FTD デバイスに展開します。
ステートフル リンクを構成すると、セカンダリ FTD は、ユーザーが接続を再確立する必要なくアクティブなセッションを引き継ぐことができるため、継続的な通信が保証されます。
参考資料:Cisco Secure Firewall Threat Defense 構成ガイド、フェールオーバー構成の章。

最新問題: **110**

別添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更新の受信に失敗しています。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を使用するように設定されています。Cisco Secure Firewall Management Centerデバイスがインテリジェンスフィード更新をダウンロードできるようにするには、どのアクションを実行すればよいですか？
A. 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。
B. Cisco Secure Firewall Management Center デバイスのプロキシ認証が無効になっていることを確認します。
C. 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。
D. intelligence.sourcefire.com のプロキシ サーバーをバイパスします。
Answer: D (メーッセージを残す)

最新問題: **111**
高可用性をサポートする 2 つの展開タイプはどれですか (2 つ選択してください)。
A. 透明
B. ルーティング
C. クラスター化された
D. シャーシ内マルチインスタンス

E. パブリッククラウド内の仮想アプライアンス
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html

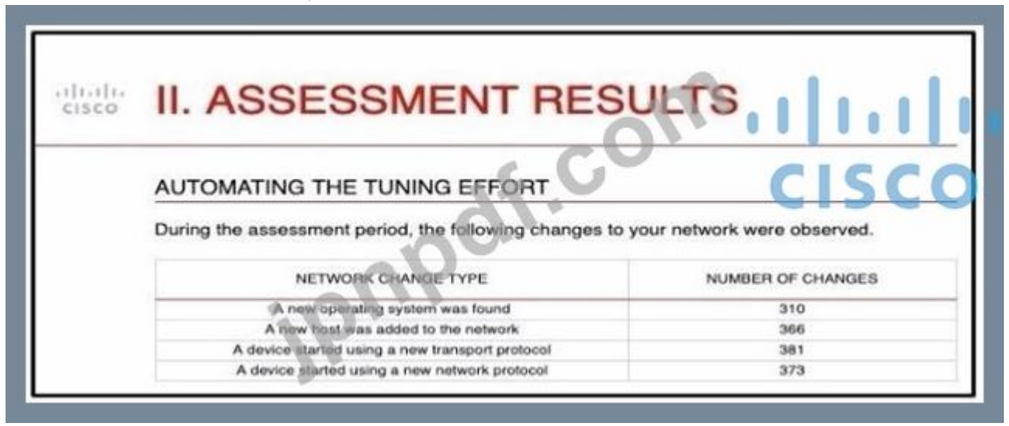
最新問題**: 112**
展示を参照してください。他のすべてのウェブサイトへの同様の通信を防ぎながら、このウェブサイトへのアクセスを修正するには、何をする必要がありますか？

```
     6: 15:46:24.605132 192.168.40.11.65830 > 172.1.1.50.80:
SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale
8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group
HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY:
FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
```

```
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-
location: frame 0x00005587afa07120 flow (NA)/NA
```

A. ポート 80 を 172.1.1.50 のみに許可するアクセス制御ポリシー ルールを作成します。
B. Snort がポート 443 を 172.1.1.50 のみに許可するように侵入ポリシー ルールを作成します。
C. ポート 443 を 172.1.1.50 のみに許可するアクセス制御ポリシー ルールを作成します。
D. Snort がポート 80 を 172.1.1.50 のみに許可するように侵入ポリシー ルールを作成します。
Answer: (解答を表示する**)**

最新問題**: 113**
展示品を参照してください。



エンジニアは攻撃リスク レポートを分析し、ネットワーク上で 300 を超える新しいオペレーティング システムのインスタンスが確認されていることを発見しました。これらの新しいオペレーティング システムを保護するために、Firepower 構成はどのように更新されるのでしょうか。
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示します。
D. 管理者がポリシーを手動で更新します。
Answer: C (メーッセージを残す**)**
説明
参照:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailori

最新問題**: 114**
インライン セット プロパティの [詳細設定] タブでは、どの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. リンク状態を伝播する
Answer: D (メーッセージを残す**)**
セクション: 展開
説明/参照: 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
最新問題**: 115**

展示を参照してください。エンジニアはアクセス制御ポーキーを変更して、ファイアウォールを通過するすべての DNS トラフィックを検査するルールを追加しています。変更を加えてポーキーを展開した後、DNS トラフィックが Snort エンジンによって完全に検査されていないことがわかりました。問題は何でしょうか。
A. ルールは検査の送信元ネットワークとポートを定義する必要があります
B. ルールのアクションは、許可ではなく信頼に設定されています。
C. ルールはトラフィックの発信元となるセキュリティゾーンを指定する必要があります
D. ルールの送信元ポートの設定が間違っています
Answer: B (メーッセージを残す**)**

最新問題**: 116**
添付資料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ファイルのどのヘッダーを設定する必要がありますか？

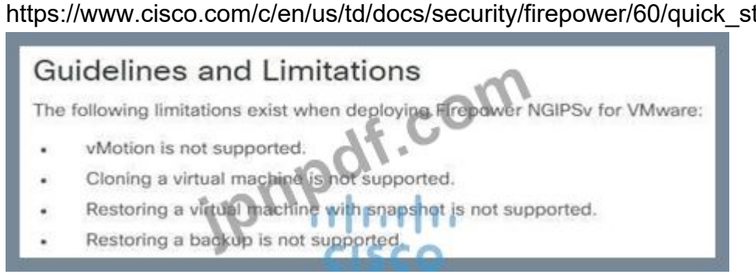
```
Network_1;Internal network;192.168.1.0/24;
FQDN_1;Domain Names;FQDN;www.example.com;ipv4_ipv6
Network_2;Internal network2;192.168.2.0/24;
```

A. 名前;説明;タイプ;値;ルックアップ;
B. 名前;説明;タイプ;値;検索;

C. 名前;説明;タイプ;値;DN;
D. 名前;説明;タイプ;値;DN;
Answer: (解答を表示する**)**
Cisco FMC のネットワーク オブジェクトの CSV インポートでは、NAME、DESCRIPTION、TYPE、VALUE などの大文字のヘッダーと、DNS ベース (FQDN) と IP ベースのオブジェクトを指定するための LOOKUP 列が必要です。

最新問題**: 117**
組織にはサーバーをクライアントから保護するためのコンプライアンス要件がありますが、クライアントとサーバーはすべて同じレイヤー 3 ネットワーク上に存在します。
クライアントまたはサーバーの IP サブネットのアドレスを再指定せずに、セグメンテーションはどのように実現されますか?
A. クライアントとサーバーの間に透過モードでファイアウォールを展開します。
B. 同じサブネット上に留まりながら、クライアントの IP アドレスを変更します。
C. クライアントとサーバーの間にルーティングモードでファイアウォールを展開する
D. 同じサブネット上に留まりながら、サーバーのIPアドレスを変更します。
Answer: A (メーッセージを残す**)**
従来、ファイアウォールはルーティングホップであり、保護されたサブネットの1つに接続するホストのデフォルトゲートウェイとして機能します。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。ただし、他のファイアウォールと同様に、インターフェース間のアクセス制御は制御されており、通常のファイアウォールチェックはすべて実施されます。レイヤ2接続は、ネットワークの内部インターフェースと外部インターフェースをグループ化した「ブリッジグループ」を使用することで実現され、Firepower Threat Defenseデバイスはブリッジング技術を使用してインターフェース間のトラフィックを通過させます。
各ブリッジグループには、ネットワーク上のIPアドレスを割り当てるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互に通信できません。

最新問題**: 118**
エンジニアが vMware 向けに Cisco Firepower NGIPSv を導入しています。
この展開中にサポートされない 2 つの側面はどれですか? (2 つ選択してください)
A. vCenter
B. バックアップの復元
C. vCloud Director
D. VMware ツール
E. 仮想マシンのクローン作成
Answer: B,E (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv- quick/intro-ngipsv.html



最新問題**: 119**
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. プラットフォームポリシー
B. アクセス制御ポリシー
C. NATポリシー
D. 侵入ポリシー
Answer: A (メーッセージを残す**)**
データプレーン インターフェイスでの SSH の有効化は、トラフィック フィルタリングや検査ではなく、インターフェイスごとの管理プロトコルを制御するプラットフォーム ポリシーによって制御されます。

最新問題: **120**
スイッチ型 Firepower デバイスの展開においてネットワーク冗長性を確立するプロトコルはどれですか?
A. STP
B. HSRP
C. GLBP
D. VRRP
Answer: A (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01101000.html

最新問題: **121**
ネットワークエンジニアがFirepower Threat DefenseでURLフィルタリングを設定しています。クラウドサービスとの通信を可能にするために、Firepower Management Centerのどの2つのポート要件を検証する必要がありますか？
（2つ選択してください。）
A. 送信ポート TCP/443
B. 受信ポート TCP/80
C. 送信ポート TCP/8080
D. 受信ポート TCP/443
E. 送信ポート TCP/80
Answer: A,E (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/SecurityInternet_Accessand_Communication_Ports.html

最新問題: **122**
Cisco FMCのイベントダッシュボードには、優先度の低い侵入ドロップイベントが大量に表示され、優先度の高いイベントが見過ごされています。エンジニアは、ポリシーを見直し、優先度の低いイベントを削減する任務を負っています。このタスクを達成するには、どのようなアクションを設定すればよいでしょうか？
A. イベントを生成する
B. パケットをドロップする
C. 接続を切断する
D. ドロップして生成

Answer: B (メーッセージを残す)
参照 :https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/working_with_intrusion_events.html

最新問題: **123**
ソフトウェア開発会社は、請負業者が社内開発者と共同で取り組んでいるプロジェクトのコードを共有するためのウェブサイト https://dev.company.com をホストしています。このウェブサーバはオンプレミスで、Cisco Secure Firewall Threat Defense アプライアンスによって保護されています。ネットワーク管理者は、このサイト経由で感染ファイルを社内ユーザーに送信しようとする人物がいるのではないかと懸念しています。Cisco Secure Firewall Malware Defense がマルウェアを検出してブロックするには、アクセス制御ポリシーにどのタイプのポリシーを関連付ける必要がありますか？
A. SSLポリシー
B. ファイルポリシー
C. ネットワーク検出ポリシー
D. プレフィルタポリシー
Answer: B (メーッセージを残す)
Cisco Secure Firewall Malware Defense が Web サーバ経由で送信されたマルウェアを検出してブロックできるようにするには、ファイル ポリシーをアクセス コントロール ポリシーに関連付ける必要があります。
ファイルポリシーとは、セキュアファイアウォールがネットワークトラフィック内のファイルにマルウェアがないか検査するために使用する設定のセットです。ファイルポリシーをアクセス制御ルールに関連付けることで、ファイアウォールはファイルを許可する前に検査を行い、送信されるファイル内のマルウェアを検出してブロックします。
これは、Web サーバー、電子メール、その他のベクトルなどのソースから発生するファイルベースの脅威を制御するために不可欠です。
https://secure.cisco.com/secure-firewall/docs/マルウェアとファイルポリシー

最新問題: **124**
エンジニアがCisco Secure Firewall Management Center内で新しいダッシュボードを設定しているのですが、カスタムウィジェットの実装に問題があります。カスタム分析ウィジェットを設定する場合、システムに情報を表示するために必須のオプションはどれですか？
A. テーブル
B. タイトル
C. フィルター
D. 結果
Answer: B (メーッセージを残す)
Cisco Secure Firewall Management Center (FMC) 内のダッシュボードでカスタム ウィジェットを設定する場合、システムが情報を正しく表示できるように、タイトルを指定することが必須です。
タイトルは、ダッシュボード上のウィジェットを識別および整理するのに役立ちます。
手順:
FMC のダッシュボード セクションに移動します。
新しいカスタム ウィジェットを追加します。
ウィジェット設定を構成し、タイトルを指定します。
ウィジェットを保存してダッシュボードに適用します。
タイトルを付けると、ウィジェットがダッシュボード上で正しく表示され、簡単に識別できるようになります。

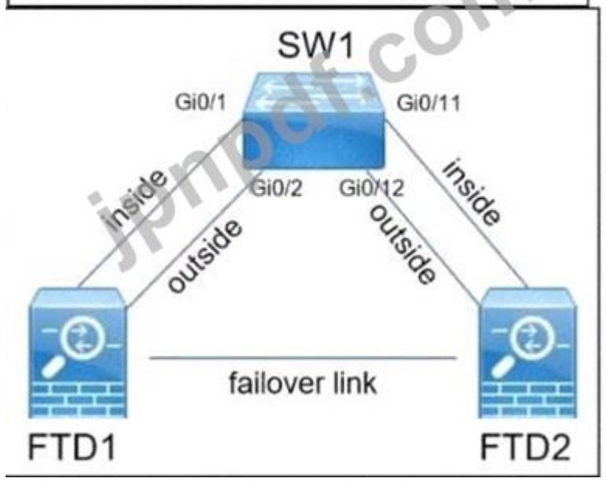
最新問題: **125**
Cisco FMC で設定され、Cisco FTD に伝播される 2 つの OSPF ルーティング機能はどれですか (2 つ選択してください)。
A. IPv6対応OSPFv2
B. 仮想リンク

C. OSPFパケットへのSHA認証
E. OSPFパケットへのMD5認証
D. エリア境界ルータタイプ1 LSAフィルタリング
Answer: B,D (メーッセージを残す)
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/ospf_for_firepower_threat_defense.html

最新問題: **126**
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. 棒グラフ
B. 矢印チャート
C. ベンチマークチャート
D. ボックスレバーチャート
Answer: A (メーッセージを残す)

最新問題: **127**
展示品を参照してください。

```
Gi0/1 and Gi0/11 configuration:
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown

Gi0/2 and Gi0/12 configuration:
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
```



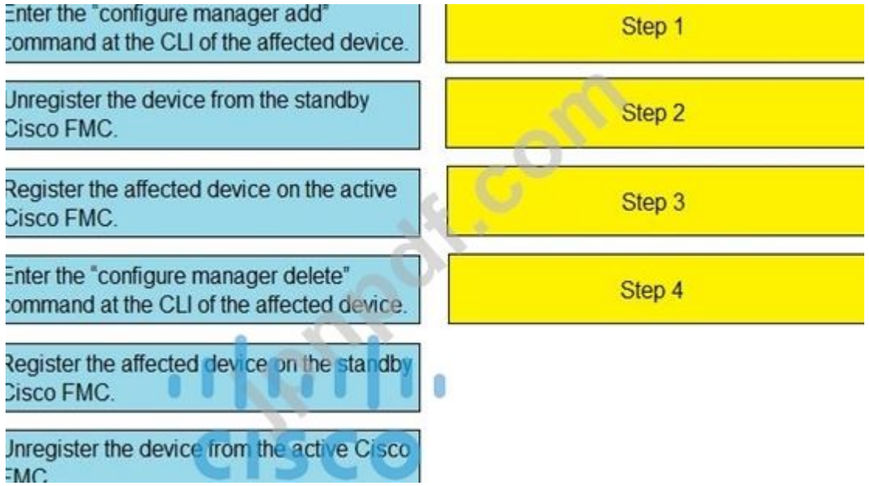
ある企業では、FTD1 と FTD2 という名前の Cisco Secure Firewall 脅威防御デバイスのペアを導入しています。
FTD1とFTD2は、フェイルオーバーリンクはあるものの、ステートフルリンクは備えていないアクティブ/スタンバイペアとして設定されています。FTD1に障害が発生した場合でも、内部ネットワーク上のユーザーが外部デバイスと通信できるようにするには、次に何を実装する必要がありますか？
A. FTD1 および FTD2 に接続されたスイッチ インターフェイスのポート セキュリティを無効にします。
B. FTD1 および FTD2 のスイッチ インターフェイスで、最大保護アドレスを 2 に設定します。
C. ステートフル リンクを接続して構成し、変更をデプロイします。

D. SW1とFTD2のスパニングツリーPortFasI機能を設定します。
Answer: C (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスを使用したフェイルオーバー構成では、プライマリデバイス（FTD1）に障害が発生した場合でも、内部ネットワーク上のユーザが外部デバイスとの通信を継続できるようにするため、ステートフルフェイルオーバーリンクを実装する必要があります。ステートフルフェイルオーバーリンクにより、セカンダリデバイス（FTD2）はセッション情報と状態データを維持できるため、シームレスなフェイルオーバーが実現し、中断を最小限に抑えることができます。
ステートフル フェイルオーバー リンクを実装する手順:
* FTD1 と FTD2 の間にステートフル フェールオーバー リンクを物理的に接続します。
* FMC でステートフル フェールオーバー リンクを設定します。
* 両方のデバイスが適切に同期され、ステートフル フェイルオーバーが有効になっていることを確認します。
* 変更を両方の FTD デバイスに展開します。
ステートフル リンクを構成すると、セカンダリ FTD は、ユーザーが接続を再確立する必要なくアクティブなセッションを引き継ぐことができるため、継続的な通信が保証されます。
参考資料:Cisco Secure Firewall Threat Defense 構成ガイド、フェールオーバー構成の章。

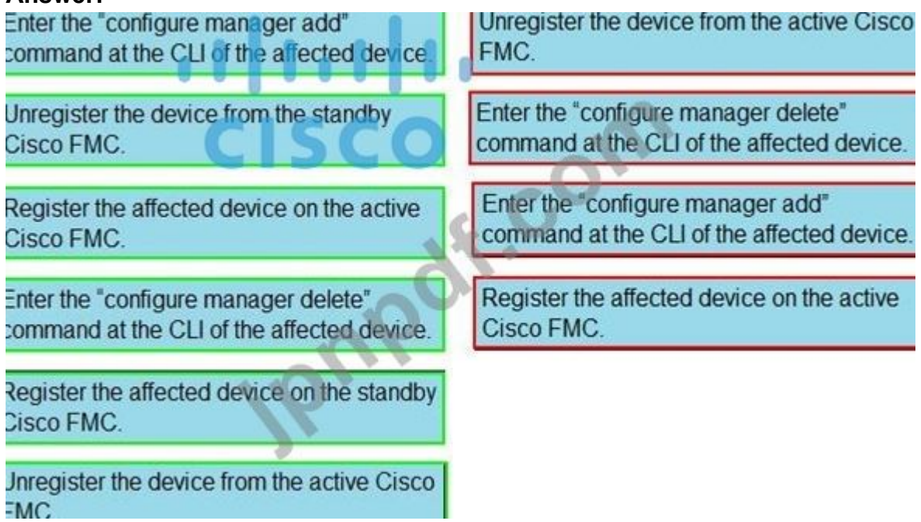
最新問題**: 128**
ネットワークエンジニアは、2台のCisco FTDデバイス間に冗長性を提供する必要があります。冗長構成には、自動構成、変換、および接続更新を含める必要があります。2台のアプライアンスの初期構成後、冗長構成を進めるために実行する必要がある2つの手順はどれですか（2つ選択してください）。
A. ステートフル プロパティを使用してフェールオーバー リンクを構成します。
B. 高可用性ライセンスが有効になっていることを確認します。
C. スタンバイ IP アドレスを設定します。
D. フェールオーバー リンクの仮想 MAC アドレスを設定します。
E. 内部インターフェースで hello を無効にします。
Answer: C,D (メーッセージを残す**)**

最新問題**: 129**
ネットワークエンジニアは、別のIPサブネットを作成せずにトラフィック検査を行うために、FTDデバイスを介してユーザーセグメントを拡張しようとしています。これは、ルーティングモードのFTDデバイスでどのように実現されるのでしょうか？
A. インラインセットインターフェースを割り当てることによって
B. BVIを使用し、ユーザーセグメントと同じサブネットにBVI IPアドレスを作成する
C. ARPを利用してトラフィックをファイアウォールに誘導する
D. 事前フィルタルールを活用してプロトコル検査をバイパスする
Answer: A (メーッセージを残す**)**
セクション: 展開

最新問題**: 130**
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。



Answer:



参照：

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

最新問題**: 131**

```
Interface: inside, Packet type: TCP, Source: 192.168.67.102, Source Port:
47381, Destination: 209.165.202.6, Destination Port: 443 (reduced output)


Phase: 1
Type: INPUT-ROUTE-LOOKUP, Subtype: Resolve Egress Interface, Result: ALLOW
Found next-hop 209.165.201.2 using egress ifc public(vrfid:0)
Phase: 2
Type: ACCESS-LIST, Subtype: log, Result: ALLOW
Config: access-list CSM_FW_ACL_ remark rule-id 268441459: RULE: Allow_HTTPS
Phase: 3
Type: CONN-SETTINGS, Result: ALLOW
Phase: 4
Type: NAT, Result: ALLOW
Config:
object network NET67
 nat (inside,public) dynamic IP67
Additional Information: Dynamic translate 192.168.67.102/47381 to 192.168.67.67/
47381
Phase: 5 - 10
Result: ALLOW
Phase: 11
Type: ADJACENCY-LOOKUP, Subtype: Resolve Nexthop IP address to MAC, Result:
ALLOW
Additional Information: Found adjacency entry for Next-hop 209.165.201.2 on
interface  public
Adjacency :Active, MAC address 000c.296c.41c3 hits 5506 reference 2

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: public(vrfid:0)
output-status: up
```

図を参照してください。IPアドレス192.168.67.102を持つクライアントが、リモートサーバーへの接続時に問題を報告しています。トポロジとパケットトレーサーツールの出力に基づいて、接続の問題を解決するにはどのアクションを実行すればよいですか？

A. クライアント側アプリケーションを再起動します。
B. FTDv のアクセス ルールをブロック解除します。
C. 宛先へのルートを追加します。
D. FTDv で NAT を再設定します。
Answer: D (メーッセージを残す**)**

最新問題: **132**
エンジニアがCisco Firepowerの特定のSGTにおける接続問題を調査しています。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するには、どのコマンドを使用すればよいですか？
A. キャプチャ CAP マッチ 64 タイプ インラインタグ ip any any
B. CAPヘッダーのみをキャプチャするタイプインラインタグ64一致IP任意任意
C. CAPバッファ64をキャプチャする ip any anyに一致
D. キャプチャ CAP タイプ インラインタグ 64 一致 IP 任意 任意
Answer: D (メーッセージを残す**)**

最新問題: **133**
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ましたが、アクセスできません。ただし、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
B. 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
C. Cisco FMC内のAPI制限によりウィジェットが表示されない
D. ウィジェットはCisco FMC内で設定されていません
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_system_user_management.html

最新問題: **134**

```
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.bbb7, MTU 1500
        Member GigabitEthernet1/5(Active), GigabitEthernet1/4
```

添付資料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 を接続し、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設定する必要があります。フェイルオーバーを設定するには、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

```
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	

Answer:

```
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
```

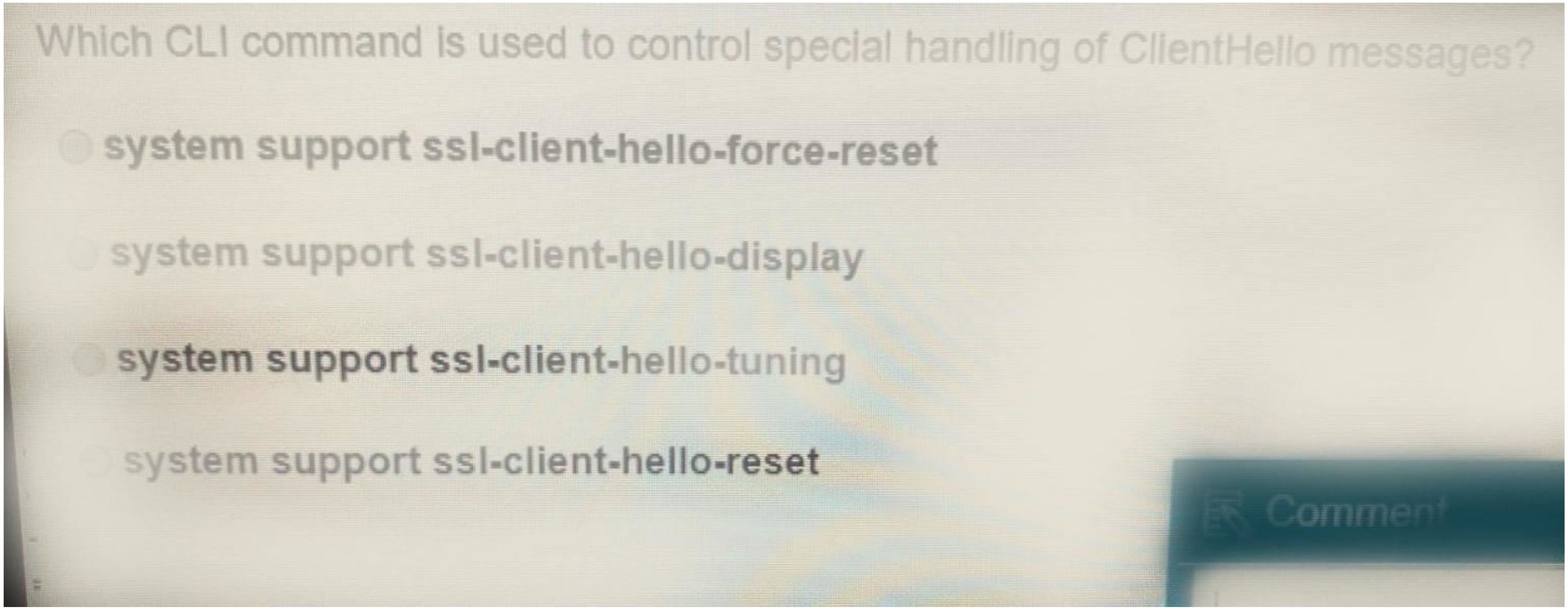
```
reactivation mode timed
```

```
failover link Redundant1 GigabitEthernet1/4
```

Explanation:

コンピューターの AI によって生成されたコンテンツのスクリーンショットは不正確である可能性があります。

最新問題: **135**
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. システムサポートは ssl-client-hello が有効です
Answer: D (メーッセージを残す**)**
説明



参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_command_line_reference.html

最新問題: **136**
FirePower Threat Defense v6.0 でサポートされている 2 つの動的ルーティング プロトコルはどれですか (2 つ選択してください)。
A. EIGRP
B. 静的ルーティング
C. OSPF
D. IS-IS
E. BGP
Answer: C,E (メーッセージを残す**)**

最新問題: **137**

高可用性の Cisco Secure Firewall Threat Defense Virtual アプライアンスのペアを Cisco Secure Firewall Management Center にどのように導入すればよいですか?
A. 最初にプライマリおよびセカンダリの Cisco Secure Firewall Threat Defense Virtual アプライアンスを Cisco Secure Firewall Management Center に追加し、次に高可用性を設定します。
B. 最初にプライマリアプライアンスを Cisco Secure Firewall Management Center に追加し、次に高可用性を設定します。
C. 最初に高可用性を設定し、次にプライマリ Cisco Secure Firewall Threat Defense Virtual アプライアンスのみを Cisco Secure Firewall Management Center に追加します。
D. 最初に高可用性を設定し、次にプライマリ アプライアンスとセカンダリ アプライアンスを Cisco Secure Firewall Management Center に追加します。
Answer: D (メーッセージを残す**)**

最新問題**: 138**
管理者は、ユーザーがクラウドホスト型Webサーバーにアクセスできないという報告を受けました。アクセス制御ポリシーは最近更新され、いくつかの新しいポリシーが追加され、URLフィルタリングも行われました。
組織のセキュリティ体制を犠牲にすることなく、問題をトラブルシューティングし、アクセスを回復するには、何を行う必要がありますか?
A. 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 モニターを含むルールを作成します。
B. 接続イベントの出力を確認してブロックを検証し、トラフィックを許可するようにポリシーを変更します。
C. トラフィックの PCAP をダウンロードしてブロックを確認し、FlexConfig を使用して既存のポリシーを上書きします。
D. Web サーバーの FQDN にポート 80 と 443 を許可する新しいアクセス制御ポリシー ルールを作成します。
Answer: B (メーッセージを残す**)**

最新問題**: 139**
展示品を参照してください。
エンジニアがアクセス制御ポリシーを変更し、通過するすべてのDNSトラフィックを検査するルールを追加しようとしたところ、変更を加えてポリシーを展開したところ、DNSトラフィックがSnortエンジンによって検査されていないことがわかりました。一体何が起こっているのでしょうか……
A. ルールでは、検査の送信元ネットワークとポートを定義する必要があります。
B. ルールでは、トラフィックの発信元となるセキュリティ ゾーンを指定する必要があります。
C. ルールのアクションは、許可ではなく信頼に設定されています。
D. ルールの送信元ポートの設定が間違っています。
Answer: C (メーッセージを残す**)**

最新問題**: 140**
マルチドメイン環境の Cisco Firepower Management Center ダッシュボードにはどのような制限が適用されますか?
A. 子ドメインは、祖先ドメインから生成されたダッシュボードを表示できますが、編集することはできません。
B. 子ドメインは、祖先ドメインの限られたウィジェット セットにのみアクセスできます。
C. 最上位の祖先ドメインの管理者だけがダッシュボードを表示できます。
D. 子ドメインは、祖先ドメインから生成されたダッシュボードを表示できません。
Answer: (解答を表示する**)**
セクション: 管理とトラブルシューティング
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Using_Dashboards.html

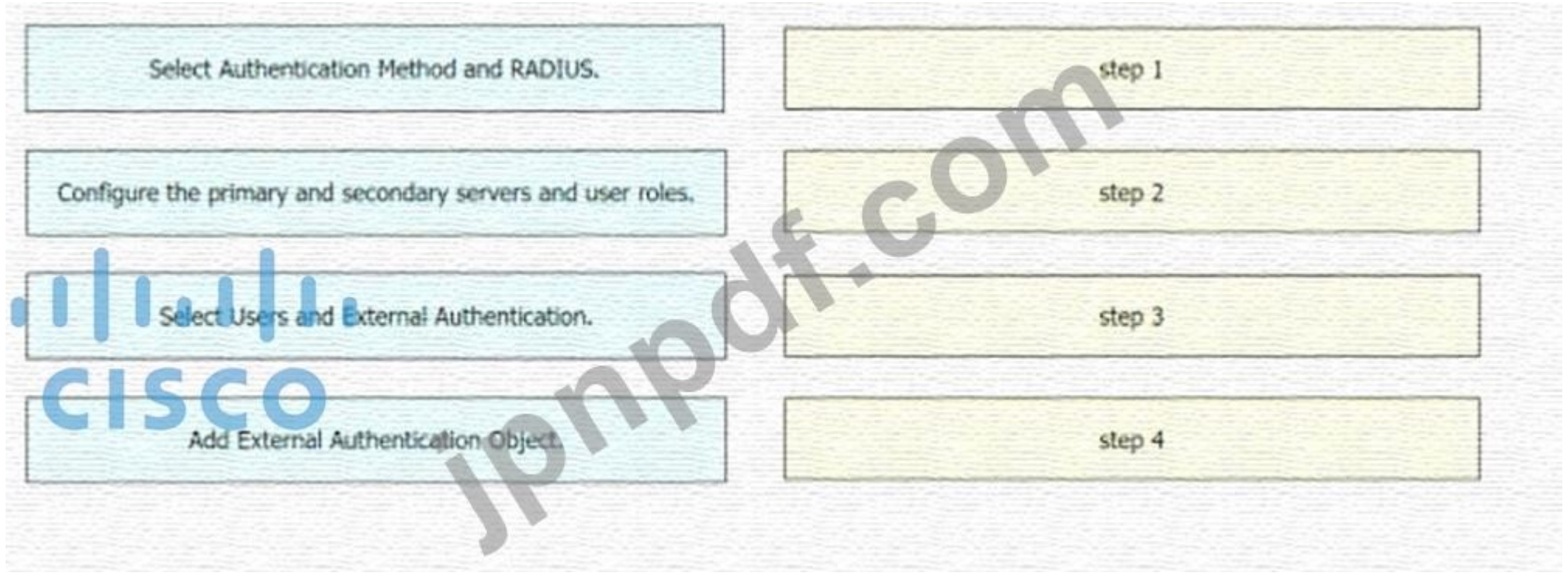
最新問題**: 141**
エンジニアは、サービスグループタグを使用しているCisco Firepowerの接続問題を調査しています。特定のデバイスが正しくタグ付けされていないため、クライアントがファイアウォールを通過する際に適切なポリシーを適用できません。この問題はどのように解決すればよいでしょうか？

A. 一致基準を使用してパケット キャプチャを使用します。
B. 高度なオプションを指定した traceroute を使用します。
C. 適切なフィルタリング機能を備えたパケットスニファーを使用する
D. IP サブネット フィルターを使用して Wireshark を使用します。
Answer: B (メーッセージを残す**)**

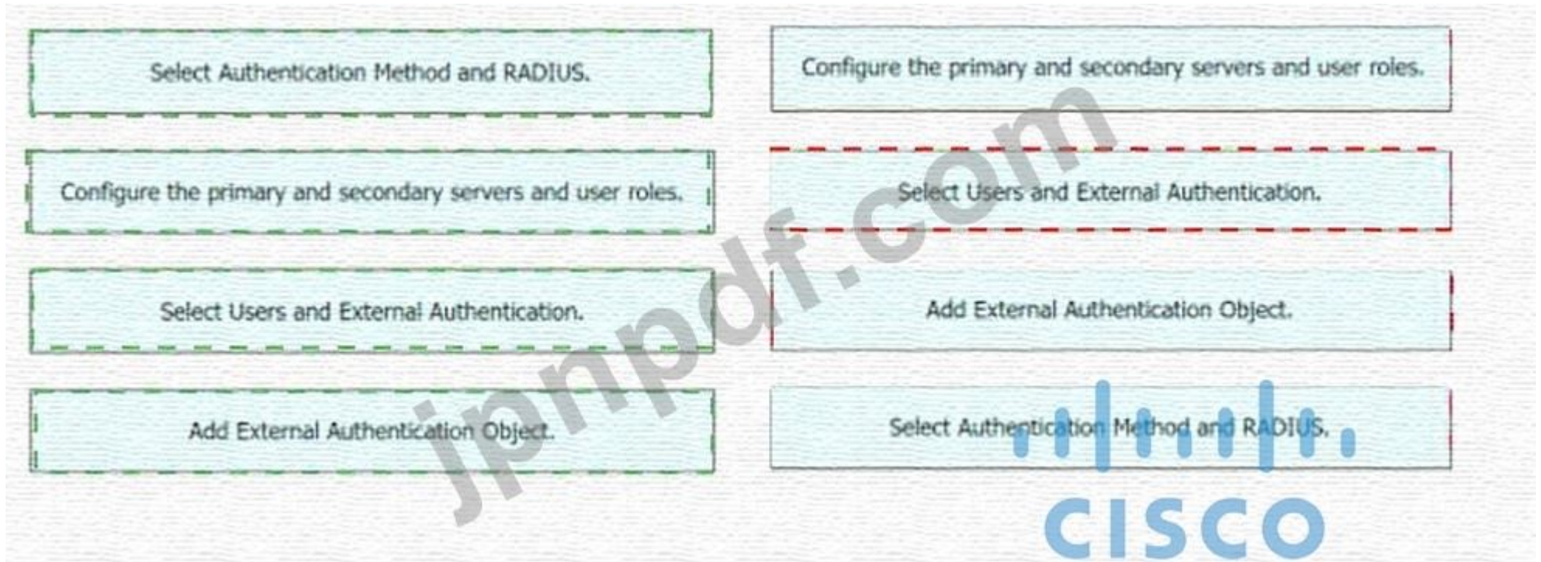
最新問題**: 142**
Cisco Firepower システムでは、アクセス制御ポリシーはどのような 2 つの方法で動作しますか? (2 つ選択してください。)
A. 構成の変更が展開されると、トラフィック検査が一時的に中断される可能性があります。
B. システムは侵入検査を実行し、その後にファイル検査を実行します。
C. セキュリティ インテリジェンス データに基づいてトラフィックをブロックできます。
D. ファイル ポリシーは、関連付けられた変数セットを使用して侵入防止を実行します。
E. システムは信頼できるトラフィックに対して予備検査を実行し、信頼できるパラメータと一致するかどうかを検証します。
Answer: (解答を表示する**)**
参考: 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

最新問題**: 143**
Cisco Secure Firewall Management Center からの標準レポートはどのファイル形式でダウンロードできますか?
A. ドキュメント
B. ppt
C. csv
D. xls
Answer: (解答を表示する**)**
Cisco Secure Firewall Management Center の標準レポートは、CSV（カンマ区切り値）形式でダウンロードできます。この形式はデータ交換に広く使用されており、Microsoft Excel などのさまざまなアプリケーションで開くことができます。
レポートをダウンロードする手順:
FMC で [レポート] > [レポート デザイナー] に移動します。
ダウンロードするレポートを選択または作成します。
レポートをエクスポートする際には、CSV形式オプションを選択してください。これにより、ネットワークエンジニアはレポートデータを簡単に分析および操作できます。

最新問題**: 144**
左側の設定手順を右側のシーケンスにドラッグ アンド ドロップして、Cisco FMC で RADIUS サーバへの外部認証を有効にします。



Answer:



Explanation:
4、1、2、3

最新問題**: 145**
アクセス制御ポリシー内で使用されるオブジェクトを編集した後、どのような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. アクセス制御ポリシーの 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。

Answer: C (メーッセージを残す)
セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

最新問題: **146**
FlexConfig を使用せずに Firepower Threat Defense でサポートされる 2 つの動的ルーティング プロトコルはどれですか。
（2つ選択してください。）
A. EIGRP
B. OSPF
C. 静的ルーティング
D. IS-IS
E. BGP
Answer: C,E (メーッセージを残す)
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

最新問題: **147**
アプリケーション層プリプロセッサにはどのようなものがありますか? (2 つ選択してください。)
A. CIFS
B. IMAP
C. SSL
D. DNP3
E. ICMP
Answer: B,C (メーッセージを残す)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html

最新問題: **148**
セキュリティエンジニアは、Cisco Secure Endpointコンソールで、SHA-256ハッシュを持つファイルに対して悪意のある判定を示すアラートを確認します。
0488537078abcdef048853abcdef048853abcdef048853abcdef048853abcdef048853。この脅威を軽減するにはどのような手順を踏めばよいでしょうか。
A. ハッシュをネットワーク ブロック リストに追加します。
B. エンドポイント上のファイルを検疫します。
C. カスタム検出リストにハッシュを追加します。
D. 感染したエンドポイントでファイアウォールを有効にします。
Answer: C (メーッセージを残す)
カスタム検出リスト > シンプル
1. SHA-256の追加オプションで、ブロックしたい特定のファイルから以前に収集したSHA-256コードを貼り付けます。
2. シンプルカスタム検出リストが生成されたら、 管理」> ポリシー」に移動し、以前に作成したリストを適用するポリシーを選択します。
https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215176-configure-a-simple-custom-detection-list.html

最新問題: **149**

ネットワーク エンジニアは、別の IP サブネットを作成せずにトラフィック検査のために FTD デバイスを介してユーザー セグメントを拡張しています。これは、ルーティング モードの FTD デバイスでどのように実現されるのでしょうか。
A. BVIを使用して、ユーザーセグメントと同じサブネットにBVI IPアドレスを作成します。
B. インラインセットインターフェースを割り当てることによって
C. 事前フィルタルールを活用してプロトコル検査をバイパスする
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html
D. ARPを利用してトラフィックをファイアウォールに誘導する
Answer: (解答を表示する**)**

最新問題**: 150**
Threat Intelligence Director がサポートするフィルタリングの最大 SHA レベルは何ですか?
A. SHA-1024
B. SHA-4096
C. SHA-512
D. SHA-256
Answer: D (メーッセージを残す**)**
セクション: 統合
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/cisco_threat_intelligence_director__tid_.html

最新問題**: 151**
セキュリティ エンジニアは、Cisco Secure Firewall Threat Defense デバイスでマルウェアおよびファイル ポリシーを作成する必要があります。
このソリューションでは、PDF、DOCX、XLSX ファイルが Cisco Secure Malware 分析に送信されないようにする必要があります。
要件を満たすために何を設定する必要があるか
A. 容量処理
B. スペロ分析
C. 動的解析
D. ローカルマルウェア分析
Answer: (解答を表示する**)**
Cisco Secure Firewall Threat Defense（FTD）デバイス上で、PDF、DOCX、XLSXファイルがCisco Secure Malware Analyticsに送信されないようにするマルウェアおよびファイルポリシーを作成するには、セキュリティエンジニアがローカルマルウェア分析を設定する必要があります。ローカルマルウェア分析により、FTDはファイルをクラウドベースのCisco Secure Malware Analyticsに送信することなく、ローカルでファイルを検査および分析できます。
ローカル マルウェア分析を構成する手順:
* FMC で、[ポリシー] > [アクセス制御] > [マルウェアとファイル ポリシー] に移動します。
* 新しいマルウェアおよびファイル ポリシーを作成するか、既存のポリシーを編集します。
* 特定のファイル タイプを検査するためのルールを定義し、PDF、DOCX、XLSX ファイルがローカルで処理されるようにします。
* これらのファイル タイプに対するアクションを 「ローカル分析」に設定します。
* 関連するアクセス制御ポリシーにポリシーを適用します。
この設定により、指定されたファイル タイプがローカルで分析され、Cisco Secure Malware Analytics に送信されないようにするという要件が満たされます。
参考資料: Cisco Secure Firewall Management Center 構成ガイド、マルウェアおよびファイル ポリシーの章

最新問題**: 152**
ある組織は、現在悪評のないウェブサイトからマルウェアがダウンロードされたことに気づきました。この問題は、どのようにすれば可能な限り迅速かつ最小限の影響で、世界規模で解決できるでしょうか？
A. Cisco Talos はポリシーを自動的に更新します。
B. ポリシーにURLオブジェクトを作成してウェブサイトをブロックする
C. アウトバウンドのWebアクセスを拒否する
D. エンドポイントを分離することで
Answer: A (メーッセージを残す**)**

最新問題**: 153**
エンジニアは、2台のCisco Secure Firewallデバイスにフェイルオーバー機能を導入しようとしています。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、ダウンタイムを最小限に抑え、ネットワークユーザーがインターネットにアクセスし続けるために、エンジニアはどのような対策を講じるべきでしょうか？
A. MAC アドレスをスイッチの ARP テーブルに追加します。
B. 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。
C. 両方のユニットに同じ MAC アドレスを設定します。
D. 両方のユニットで仮想MACアドレスを使用する
Answer: D (メーッセージを残す**)**

最新問題**: 154**
エンジニアはCisco Firepowerデバイスの高可用性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台のデバイスが同時にトラフィックを通過させることができません。この環境ではデバイスをどのように実装する必要がありますか?
A. クラスタインターフェースモード
B. アクティブ/パッシブモード
C. クラスタスパンEtherChannel内
D. アクティブ/アクティブモード
Answer: (解答を表示する**)**

最新問題**: 155**
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. 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
C. マルチドメインシステムに現在のドメインを含める
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
Answer: C (メーッセージを残す**)**
FMC のリスク レポートはドメイン コンテキストごとに生成され、マルチドメイン階層全体ではなく、アクティブな (現在の) ドメイン内のオブジェクトとイベントのみが対象となります。
最新問題**: 156**
FlexConfig を使用せずに Firepower Threat Defense でサポートされる動的ルーティング プロトコルはどれですか (2 つ選択してください)。

A. EIGRP
B. BGP
C. OSPF
D. 静的ルーティング
E. IS-IS
Answer: B,C (メーッセージを残す**)**

最新問題**: 157**
スイッチ型 Firepower デバイスの展開においてネットワーク冗長性を確立するプロトコルはどれですか?
A. STP
B. HSRP
C. GLBP
D. VRRP
Answer: A (メーッセージを残す**)**
セクション: 展開
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_threat_defense_high_availability.html

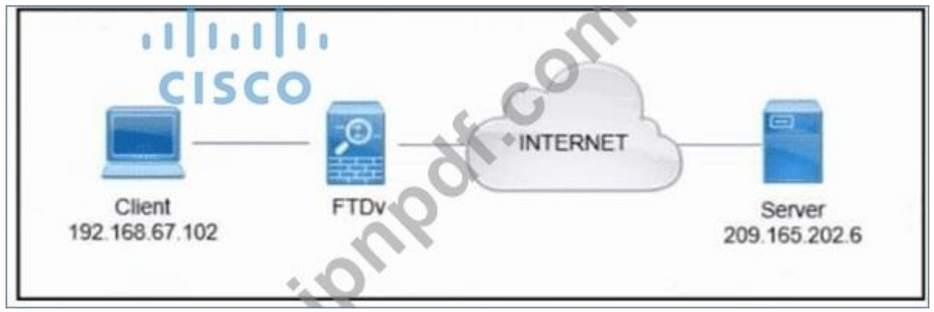
最新問題**: 158**
エンジニアはCisco FTDデバイスを導入する必要があります。経営陣は、エンドユーザーに影響を与えるネットワーク変更を必要とせずにトラフィックを検査したいと考えています。企業のセキュリティポリシーでは、管理トラフィックとデータトラフィックを分離し、リモート管理にはTelnet経由のSSHを使用することが義務付けられています。これらの要件を満たすには、デバイスをどのように導入すればよいでしょうか？
A. 診断インターフェースを備えたルーティングモード
B. 管理インターフェースを備えた透過モード
C. データインターフェースで作成された透過的な
D. ブリッジ仮想インターフェースを使用したルーティングモード
Answer: (解答を表示する)
説明
質問の要件を満たすCisco FTDデバイスを導入するには、エンジニアは管理インターフェイスを備えたトランスペアレントモードを使用する必要があります。トランスペアレントモードとは、FTDデバイスが「Bump In The Wire」または「ステルスファイアウォール」として機能し、接続されたデバイスへのルータホップとして認識されないファイアウォール設定です。トランスペアレントモードでは、FTDデバイスは、IPアドレスやルーティング設定の変更など、エンドユーザに支障をきたすネットワーク変更を必要とせずにトラフィックを検査できます1。管理インターフェイスは、FTDデバイスの管理と管理トラフィックとデータトラフィックの分離に使用される専用インターフェイスです。管理インターフェイスは、Telnetよりも安全なリモート管理用のSSHアクセスを許可するように設定できます2。
その他のオプションは、次の理由により正しくありません。
ルーテッドモードは、FTDデバイスがルータとして機能し、接続されたネットワークのアドレス変換とルーティングを実行するファイアウォール設定です。ルーテッドモードでは、IPアドレスやルーティング設定の変更など、エンドユーザに支障をきたす可能性のあるネットワーク変更が必要になります1。診断インターフェイスは、FTDデバイス上のトラフィックのトラブルシューティングとキャプチャに使用される特別なインターフェイスです。診断インターフェイスは、管理トラフィックとデータトラフィックを分離したり、リモート管理用のSSHアクセスを許可したりしません。
データインターフェースを備えた透過モードでは、管理トラフィックとデータトラフィックを分離するという要件を満たしていません。データインターフェースは、FTDデバイス上でトラフィックの通過と検査に使用される通常のインターフェースです。トランスペアレントモードでは、エンドユーザに支障をきたすネットワーク変更を必要とせずにトラフィックを検査するという要件を満たしていません。BVIは、同じレイヤ2ブロードキャストドメインに属する1つ以上の物理または論理インターフェイスのコンテナとして機能する論理インターフェイスです。BVIを使用すると、FTDデバイスは同じセキュリティモジュール/エンジン上の異なるブリッジグループ間でルーティングを行うことができます。ただし、ルーテッドモードでは、IPアドレスやルーティング設定の変更など、エンドユーザに支障をきたす可能性のあるネットワーク変更が必要になります。

最新問題: **159**
Cisco Threat Response を使用する場合、インテリジェンス サイクルのどのフェーズ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
Answer: B (メーッセージを残す)
配布: 配布フェーズでは、調査または脅威ハンティングの結果を公開します。
この情報は、情報の受信者に焦点を当てて伝達されます。戦術レベルでは、この情報はF3EADモデルの根幹であるFindにフィードバックされます。図3はF3EADモデルを示しています。

最新問題: **160**
Cisco FMC が Cisco ISE と統合されている場合、使用できる修復オプションは 2 つありますか (2 つ選択してください)。
A. 動的ヌルルートが設定されました
B. DHCPプールの無効化
C. 隔離
D. ポートのシャットダウン
E. ホストのシャットダウン
Answer: C,D (メーッセージを残す)
参照：
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure- firepower-6-1-pxgrid-remediati.html

最新問題: **161**

```
1  FMC: System > Monitor > [FTDv] > Advanced Troubleshooting > Packet Tracer
2
3  Interface: inside, Packet type: TCP, Source: 192.168.67.102, Source Port:
•  47381, Destination: 209.165.202.6, Destination Port: 443 (reduced output)
4
5
6  Phase: 1
7  Type: INPUT-ROUTE-LOOKUP, Subtype: Resolve Egress Interface, Result: ALLOW
8  Found next-hop 209.165.201.2 using egress ifc  public(vrfid:0)
9  Phase: 2
10 Type: ACCESS-LIST, Subtype: log, Result: ALLOW
11 Config: access-list CSM_FW_ACL_ remark rule-id 268434451: RULE: Allow_HTTPS
12 Phase: 3
13 Type: CONN-SETTINGS, Result: ALLOW
14 Phase: 4
15 Type: NAT, Result: ALLOW
16 Config:
17 object network NET67
18  nat (inside,public) dynamic IP67
19 Additional Information: Dynamic translate 192.168.67.102/47381 to 192.168.67.67/
•  47381
20 Phase: 5 to 10
21 Result: ALLOW
22 Phase: 11
23 Type: ADJACENCY-LOOKUP, Subtype: Resolve Nexthop IP address to MAC, Result:
•  ALLOW
24 Additional Information: Found adjacency entry for Next-hop 209.165.201.2 on
•  interface  public
25 Adjacency :Active, MAC address 000c.296c.41c3 hits 5506 reference 2
26
27 Result:
28 input-interface: inside(vrfid:0)
29 input-status: up
30 input-line-status: up
31 output-interface: public(vrfid:0)
32 output-status: up
33 output-line-status: up
```



図を参照してください。IPアドレス192.168.67.102を持つクライアントが、リモートサーバーへの接続時に問題を報告しています。トポロジとパケットトレーサーツールの出力に基づいて、接続の問題を解決するにはどのアクションを実行すればよいですか？

A. 宛先へのルートを追加します。
B. FTDv で NAT を再設定します。
C. クライアント側アプリケーションを再起動します。
D. FTDv のアクセス ルールをブロック解除します。
Answer: (解答を表示する**)**

最新問題: **162**
次世代ファイアウォールの IRB 機能の目的は何ですか?
A. 2つのレイヤ2インターフェース間の透過ブリッジングを有効にする
B. 2つのレイヤー3インターフェース間のルーティングをブロックする
C. NATを透過モードで設定するには
D. 複数の物理インターフェースを同じVLANに組み込むことを許可する
Answer: A (メーッセージを残す**)**

最新問題: **163**
トラブルシューティング ファイルを生成するには、Cisco FMC CLI でどのコマンドを入力しますか?
A. 実行中の設定を表示
B. テクニカルサポートシャーシの表示
C. システムサポート診断 CLI
D. sudo sf_troubleshoot.pl
Answer: D (メーッセージを残す**)**
トラブルシューティング ファイルを生成するには、Firepower Management Center で次のコマンドを入力します。
管理者@FMC:~$ sudo sf_troubleshoot.pl
https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

最新問題: **164**
Cisco UmbrellaとCisco Threat Responseを統合する際に、ネットワークセキュリティエンジニアは、Cisco Threat ResponseインターフェースからCisco Umbrellaへドメインのブロックを自動的にプッシュしたいと考えています。この要件を満たすAPIはどれですか？
A. 報告
B. 調査する

C. REST
D. 強制
Answer: (解答を表示する**)**

最新問題: **165**
Rapid Threat Containment のために Cisco ISE と Cisco FMC を統合するために使用されるコネクタはどれですか?
A. pxGrid
B. FTD RTC
C. ISEグリッド
D. FMC RTC
Answer: A (メーッセージを残す**)**

最新問題: **166**
コンサルタントは、顧客がFDMで管理する単一のCisco Firepower 2130から、高可用性を実現するためにFMCで管理される2台のCisco Firepower 2130にアップグレードするプロジェクトに携わっています。顧客は、FDMで管理されている既存のデバイスの設定をFMCに引き継ぎ、追加するデバイスに複製することで高可用性ペアを構築することを希望しています。この要件を満たすために、コンサルタントはどのような対応を取る必要がありますか？
A. デバイスを登録する前に、現在の FDM 構成を FMC に手動で設定する必要があります。
B. デバイスの登録時に、現在の FDM 構成が自動的に FMC に変換されます。
C. 現在の FDM 設定は、セキュア ファイアウォール移行ツールを使用して FMC に移行する必要があります。
D. FTD 設定を ASA コマンド形式に変換し、FMC に移行する必要があります。
Answer: B (メーッセージを残す**)**
FDM によって管理されている FTD デバイスが FMC に登録されると、既存の設定が自動的に変換され、FMC にインポートされます。その後、FMC は設定をデバイスにプッシュします。
このプロセスでは、VPN ウィザードや証明書など、FMC でサポートされていない一部の機能を除き、FDM 設定の大部分が保持されます。

最新問題: **167**
ネットワークエンジニアがCisco AMP for Endpointsコンソールにログインし、特定されたSHA-256ハッシュが悪意のあるものと判定されたことを確認しました。この脅威を軽減するには、どのような設定が必要ですか？
A. 感染したエンドポイントからのハッシュをネットワーク ブロック リストに追加します。
B. 単純なカスタム削除リストにハッシュを追加します。
C. 正規表現を使用して悪意のあるファイルをブロックします。
D. 感染したエンドポイントでパーソナル ファイアウォールを有効にします。
Answer: (解答を表示する**)**

最新問題: **168**
エンジニアは、接続問題のトラブルシューティングを行うために、Cisco FTDでパケットキャプチャを実行し、IPアドレス192.168.100.100を使用するホストのMACアドレスが1234.5678.901であることを確認した

いと考えています。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 送信元 192.168.100.100
B. -src 192.168.100.100 なし
C. -w キャプチャ.pcap -s 1518 ホスト 192.168.100.100 mac
D. -w capture.pcap -s 1518 ホスト 192.168.100.100 イーサ
Answer: B (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working- with-firepower-threat-defense-f.html

最新問題**: 169**
エンジニアは、Cisco Secure Firewall Management Center を使用して、Cisco Secure IPS にインラインセットを設定する必要があります。インラインセットは、パケットを分析する前に各パケットのコピーを作成し、3ウェイハンドシェイクを完了しない接続をブロックする必要があります。以下の設定はすでに実施済みです。
* インライン セットに追加するインターフェイスを選択して有効にします。
* 速度とデュプレックスを設定します。
* インライン セットを設定し、インターフェイスをインライン セットに追加します。
どのアクションでタスクが完了しますか?
A. リンク ステート プロパゲーションを構成します。
B. 厳密な TCP 強制を実装します。
C. Snort フェールオープンを設定します。
D. タップ モードをインラインに設定します。
Answer: B (メーッセージを残す**)**
Cisco Firepower Management Center はいくつのレポート テンプレートをサポートしていますか?
A. 20
最新問題**: 170**
B. 10
C. 5
D. 無制限
Answer: (解答を表示する**)**
セクション: 管理とトラブルシューティング
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Working_with_Reports.html

最新問題**: 171**
エンジニアは、Cisco Secure Firewall Management Center を使用している各部門のネットワークへの ICMP トラフィックを拒否する必要があります。エンジニアは、各ネットワークの関連デバイスで同じオブジェクトを使用する必要があります。Secure Firewall Management Center ではどのような設定が必要ですか？
A. IP範囲
B. オーバーライドを許可するチェックボックス
C. IPアドレス
D. ICMPを拒否するチェックボックス
Answer: B (メーッセージを残す**)**

最新問題**: 172**
エンジニアがCisco FMCでCisco FTDデバイスのURLフィルタリングを設定しています。ユーザーがhttp:/'www.Dac'additstte.cornにアクセスする際に警告が表示され、必要に応じてウェブサイトへのアクセスを続行できるオプションが表示される必要があります。

他のウェブサイトはブラックアウトしてはいけません。エンジニアはこれらの要件を満たすために、どの2つのアクションを実行する必要がありますか？
（2つ選択してください。）
A. アクセス制御ポリシー エディターの [HTTP 応答] タブで、[ブロック応答ページ] を [カスタム] に設定します。
B. アクセス制御ポリシー エディターの [HTTP 応答] タブで、インタラクティブ ブロック応答ページをシステム提供に設定します。
C. アクセス制御ポリシーのデフォルトのアクションをインタラクティブ ブロックに設定します。
D. アダルト URL カテゴリに一致するアクセス制御ルールを設定し、アクションをインタラクティブ ブロックに設定します。
E. http://www.badaduitslte.com の URL オブジェクトに一致するアクセス制御ルールを設定し、アクションをインタラクティブ ブロックに設定します。
Answer: B,E (メーッセージを残す)
Cisco FMC で Cisco FTD デバイスの URL フィルタリングを設定し、質問の要件を満たすには、エンジニアは次の操作を行う必要があります。
* アクセス制御ポリシーエディタの 「HTTPレスポンス」タブで、「インタラクティブブロックレスポンスページ」を 「システム提供」に設定します。これにより、ユーザーがブロックされたURLにアクセスしようとした際に警告ページが表示され、続行またはキャンセルの選択肢が提供されます。システム提供ページは、一般的なメッセージとロゴ1を含むデフォルトのページです。
* 設定
http://www.badadultsite.com の URL オブジェクトに一致するアクセス制御ルールを作成し、アクションを 「インタラクティブブロック」に設定します。これにより、URL オブジェクトで定義された特定の URL にインタラクティブブロックアクションが適用されます。
インタラクティブ ブロック アクションは、前の手順 1 で構成されたインタラクティブ ブロック応答ページをトリガーします。
その他のオプションは、次の理由により正しくありません。
* アクセス制御ポリシーエディタの 「HTTPレスポンス」タブで、「ブロックレスポンスページ」を 「カスタム」に設定しても、インタラクティブブロックアクションには影響しません。ブロックレスポンスページは、アクションが 「インタラクティブブロック1」ではなく 「ブロック」に設定されている場合に使用されます。
* アクセス制御ポリシーのデフォルトアクションを 「インタラクティブブロック」に設定すると、どのアクセス制御ルールにも一致しないすべてのURLにインタラクティブブロックが適用されます。これは、 「他のウェブサイトをブロックしない」という要件を満たしません1。
* アダルト URL カテゴリに一致し、アクションをインタラクティブ ブロックに設定するアクセス制御ルールを構成すると、アダルト カテゴリに属するすべての URL にインタラクティブ ブロック アクションが適用されます。
これ
http://www.badadultsite.com のみをブロックするという要件を満たしません
1.

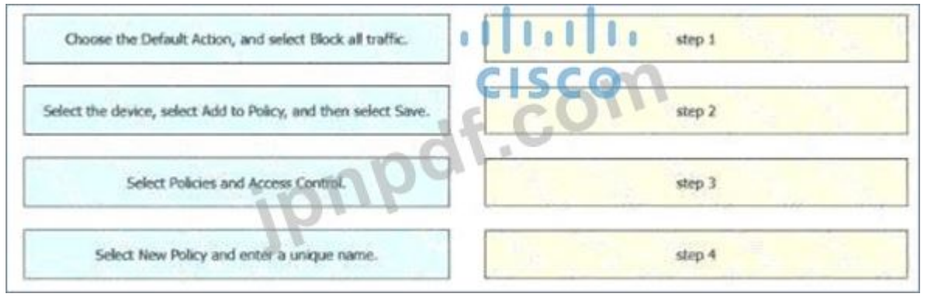
最新問題: **173**
Cisco Secure Firewall Threat Defense リモート アクセス VPN で使用できる 2 つの機能はどれですか。
（2つ選択してください。）
A. ゼロタッチネットワーク展開のためのライセンス利用
B. RADIUS動的認証を使用したRapid Threat Containmentのサポート
C. LDAPSを使用してDuoの2要素認証を有効にする
D. SSL リモート アクセス VPN は、SSL ポート 443 を使用して他の Cisco FTD 機能とのポート共有をサポートします。
E. クラスタモードでのCisco Secure Firewall 4100シリーズのサポート
Answer: (解答を表示する)

最新問題: **174**
Cisco AMP for Endpoints のどの 2 つの機能により、アップロードされたファイルをブロックできますか? (2 つ選択してください。)
A. アプリケーションのブロック
B. シンプルなカスタム検出

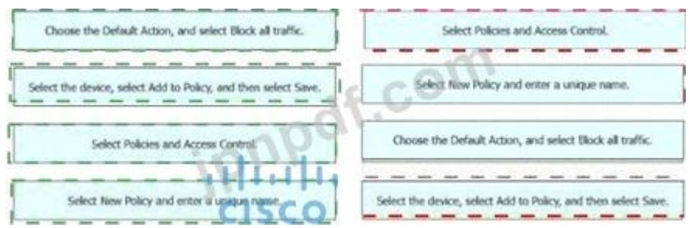
C. ファイルリポジトリ
D. 除外
E. アプリケーションのホワイトリスト
Answer: A,B (メーッセージを残す**)**
組織全体に対してカスタム マルウェア検出ポリシーとプロファイルを構成し、すべてのユーザーのファイルに対してフラッシュ スキャンとフル スキャンを実行し、ヒート マップ、詳細なファイル情報、ネットワーク ファイルの軌跡、脅威の根本原因の表示を含むマルウェア分析を実行し、自動隔離、隔離されていない実行可能ファイルの実行を停止するアプリケーション ブロック、除外リストなど、アウトブレイク制御の複数の側面を構成します。
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#id_96014

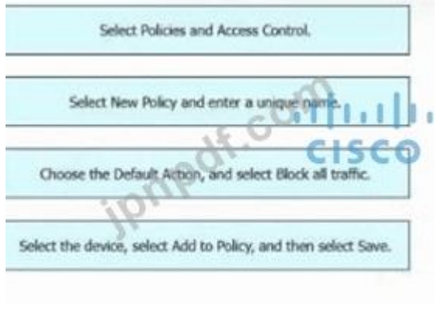
最新問題**: 175**
管理対象デバイスをインラインで展開するための最小要件は何ですか?
A. インラインインターフェース、セキュリティゾーン、MTU、モード
B. パッシブインターフェース、MTU、モード
C. インラインインターフェース、MTU、モード
D. パッシブインターフェース、セキュリティゾーン、MTU、モード
Answer: C (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html

最新問題**: 176**
エンジニアは、Cisco Secure Firewall Management Center で基本的なアクセス制御ポリシーを作成し、デフォルトですべてのトラフィックをブロックする必要があります。左側の設定アクションを右側のシーケンスにドラッグ＆ドロップします。



Answer:





最新問題: **177**
Snort エンジンがダウンしている場合やパケットの処理に時間がかかりすぎる場合に備えてパケット バイパスが設定されている場合、Cisco FMC でどのアクションを実行する必要がありますか?
A. 自動アプリケーションバイパスを有効にする
B. 検査をバイパスするためのFastpathルールを設定する
C. 障害時のバイパスしきい値ポリシーを追加する
D. ローカルルータ トラフィックの検査を有効にする
Answer: (解答を表示する**)**

最新問題: **178**
Cisco FMC が HTTPS 証明書に対してサポートする最大ビット サイズはどれくらいですか?
A. 1024
B. 8192
C. 4096
D. 2048
Answer: D (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/system_configuration.html

最新問題: **179**
セキュリティエンジニアは、組織のSyslogサーバイベントを確認したところ、Cisco Secure Endpointを実行しているホストから悪意のあるサイトへのアウトバウンド接続が多数発生していることを確認しました。これらのホストは、Cisco FTDデバイスとは別のネットワーク上に存在します。これらの接続をブロックするには、どのようなアクションが必要ですか？
A. Cisco Secure Endpoint のポリシーを変更して、DFC を有効にします。
B. Cisco FMCのアクセス制御ポリシーを変更して、悪意のあるアウトバウンド接続をブロックします。
C. 悪意のあるサイトのIPアドレスをCisco FMCのアクセス制御ポリシーに追加します。
D. TetraおよびSperoエンジンを有効にしたCisco Secure Endpointポリシーを追加します。
Answer: A (メーッセージを残す**)**
DFC が有効になっている Cisco Secure Endpoint は、エンドポイントが Cisco Firepower Threat Defense（FTD）デバイスとは別のネットワーク上にある場合でも、デバイスのネットワーク フローを相関させ、エンドポイントで直接ブロックを適用することで、悪意のあるアウトバウンド接続をブロックできます。
Cisco FMC (Firepower Management Center) のアクセス制御ポリシーを変更したり、FMC ポリシーに IP アドレスを追加したりしても、FMC/FTD が直接制御しない別のネットワーク上のホストからの接続はブロックされません。
Secure Endpoint で DFC を有効にすると、エンドポイント エージェントは脅威インテリジェンスとポリシーに基づいて悪意のある IP またはドメインへの接続をブロックできるようになります。これは、FTD のネットワーク範囲外のホストに対して効果的です。
https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf (73 ページ)

最新問題: **180**
エンジニアがCisco FMCを設定しており、複数の物理インターフェースを同じVLANに接続できるようにしたいと考えています。管理対象デバイスは、サブインターフェースを含むインターフェース間でレイヤ2スイッチングを実行できる必要があります。これらの要件を満たすには、どのような設定が必要ですか？
A. インターフェースベースのVLANスイッチング
B. シャーシ間クラスタリングVLAN
C. Cisco ISE セキュリティ グループ タグ
D. 統合ルーティングとブリッジング
Answer: D (メーッセージを残す**)**

最新問題: **181**
FTDユニットをIPアドレスのFMCマネージャに関連付けるためにFTDユニットで実行されるコマンドはどれですか？
10.0.0.10 で、登録キーは Cisco123 ですか?
A. マネージャのローカル 10.0.0.10 Cisco123 を設定します
B. マネージャの設定にCisco123 10.0.0.10を追加します
C. マネージャのローカル Cisco123 10.0.0.10 を設定します。
D. マネージャの設定に 10.0.0.10 Cisco123 を追加します
Answer: D (メーッセージを残す**)**
セクション: 構成
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt- nw.html#id_106101

最新問題: **182**
エンジニアは、Cisco Secure Firewall Management Center 上でカスタム侵入ルールを設定し、文字列 「04 68 72 80 87 ff ed cq fg he qm pn|」を含む特定のペイロードを持つ悪意のあるトラフィックパターンを検出してブロックする任務を負っています。エンジニアは IPS ポリシーでどのアクションを設定する必要がありますか？
A. 隔離
B. 無効にする
C. 警告
D. ドロップ
E. リセット
Answer: (解答を表示する**)**

最新問題: **183**
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ースを使用して、トランスペアレントファイアウォールモードで動作しています。パケットトレースの宛先MACアドレスを指定するエンジニアは、どのような点に留意すべきでしょうか？
A. UDP パケット タイプのみがサポートされます。
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. VLAN ID 値が入力されている場合、宛先 MAC アドレスはオプションです。
D. VLAN ID と宛先 MAC アドレスはオプションです。
Answer: C (メーッセージを残す**)**

最新問題: **184**
ネットワークエンジニアはCisco Firepower 4100アプライアンスを導入しており、高可用性を実現するためにマルチインスタンス環境を構成する必要があります。左側のアクションを右側のシーケンスにドラッグ

Answer:

説明
Cisco Firepower 4100 アプライアンスで高可用性を実現するマルチインスタンス環境を構成するための正しいアクションのシーケンスは次のとおりです。
コンテナインスタンスのリソースプロファイルを追加します。リソースプロファイルは、各コンテナインスタンスのCPU、RAM、ディスク容量の割り当てを定義します。異なるリソース設定を持つ複数のリソースプロファイルを作成し、それらを異なるコンテナインスタンスに割り当てることができます1。
MAC プールプレフィックスを追加し、コンテナインスタンスインターフェースの MAC アドレスを表示します。MAC プールプレフィックスは、コンテナインスタンスインターフェースの MAC アドレスを生成するために使用される 24 ビットのプレフィックスです。
カスタムMACプールプレフィックスを指定するか、デフォルトのプレフィックスを使用できます。また、各コンテナインスタンスインターフェース1に割り当てられているMACアドレスを確認することもできます。
インターフェースを設定します。コンテナインスタンスが使用する物理インターフェース、EtherChannel、およびVLANサブインターフェースを設定する必要があります。また、同じセキュリティモジュール/エンジン1上の複数のコンテナインスタンスで使用できる共有インターフェースを設定することもできます。

Cisco Secure Firewall Management Center にスタンドアロンの Firepower Threat Defense を追加します。スタンドアロンの Firepower Threat Defense (FTD) アプリケーションインスタンスを実行する論理デバイスを追加し、Cisco Secure Firewall Management Center (FMC) に登録する必要があります。この論理デバイスは、コンテナインスタンス1 の管理インターフェイスとして機能します。
高可用性ペアを追加します。スタンドアロンの FTD アプリケーションインスタンスを実行する別の論理デバイスを追加し、FMC に登録する必要があります。次に、2 つのスタンドアロン FTD 論理デバイス間に高可用性 (HA) を設定する必要があります。これにより、それらに関連付けられているコンテナインスタンスの HA が有効になります1。

最新問題: **185**

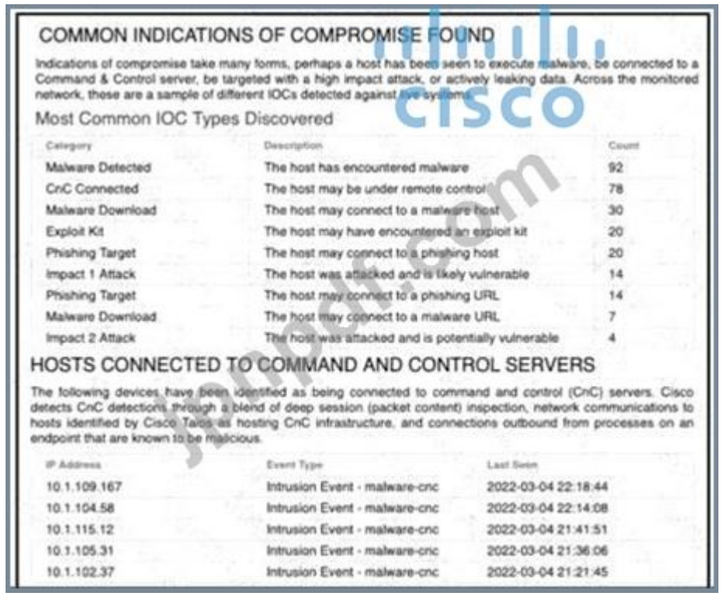
Cisco Firepower システムでは、アクセス制御ポリシーはどのような 2 つの方法で動作しますか? (2 つ選択してください。)

A. 構成の変更が展開されると、トラフィック検査が一時的に中断されます。
B. システムは侵入検査を実行し、その後に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します。
D. ファイル ポリシーは、関連付けられた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に対して予備検査を実行し、信頼できるパラメータと一致するかどうかを検証します。

Answer: A,C (メーッセージを残す**)**

セクション: 構成
説明/参照: 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

最新問題: **186**



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ます。リスクを軽減するために、エンジニアはどのような実装を推奨すべきでしょうか？

A. ネットワークベースの検出
B. 仮想保護
C. トレンド分析
D. IPアドレスとURLのブラックリスト

Answer: A (メーッセージを残す**)**

最新問題: **187**

アナリストは、ネットワーク内の侵害の可能性があるエンドポイントを調査しており、問題のエンドポイントのホストレポートを取得してメトリクスとドキュメントを収集しています。調査のために、このレポー

トからどのような情報を取得すべきでしょうか？

A. 侵入イベント、ホスト接続、およびユーザーセッション

B. 攻撃を受けたマシンの数、攻撃元、トラフィックパターン

C. 時間の経過に伴う脅威の検出とマルウェアを転送するアプリケーションプロトコル

D. ユーザー別のクライアント アプリケーション、Web アプリケーション、およびユーザー接続

Answer: (解答を表示する**)**

最新問題: **188**

管理者はCisco ASAからCisco FTDアプライアンスへの移行作業を進めており、トラフィックを中断することなく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ればよいでしょうか？

A. アクセス制御

B. プレフィルター

C. アイデンティティ

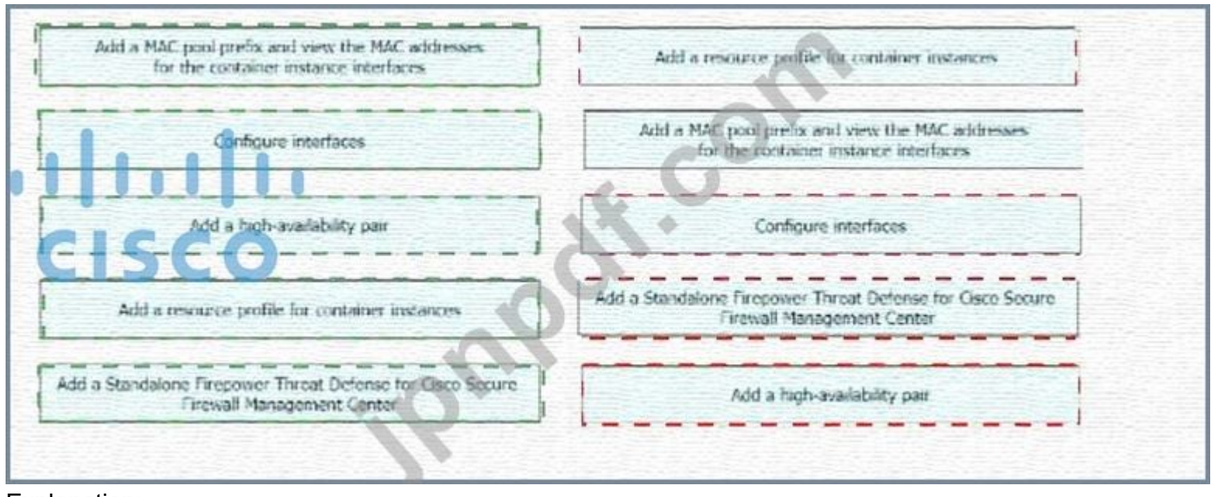
D. 侵入

Answer: A (メーッセージを残す**)**

最新問題: **189**

ネットワークエンジニアはCisco Firepower 4100アプライアンスを導入しており、高可用性を実現するためにマルチインスタンス環境を構成する必要があります。左側のアクションを右側のシーケンスにドラッグ＆ドロップして、この構成に追加してください。

Answer:



Explanation:

Cisco Firepower 4100 アプライアンスで高可用性を実現するマルチインスタンス環境を構成するための正しいアクションのシーケンスは次のとおりです。

* コンテナインスタンスのリソースプロファイルを追加します。リソースプロファイルは、各コンテナインスタンスのCPU、RAM、ディスク容量の割り当てを定義します。異なるリソースプロファイルを複数作成できます。

* 設定を別のコンテナ インスタンスに割り当てます1。

* MAC プールプレフィックスを追加し、コンテナインスタンスインターフェースの MAC アドレスを表示します。MAC プールプレフィックスは、コンテナインスタンスインターフェースの MAC アドレスを生成するために使用される 24 ビットのプレフィックスです。

カスタムMACプールプレフィックスを指定するか、デフォルトのプレフィックスを使用できます。また、各コンテナインスタンスインターフェース1に割り当てられているMACアドレスを確認することもできます。

* インターフェイスを設定します。コンテナインスタンスが使用する物理インターフェイス、EtherChannel、およびVLANサブインターフェイスを設定する必要があります。また、同じセキュリティモジュール/エンジン1上の複数のコンテナインスタンスで使用できる共有インターフェイスを設定することもできます。

* Cisco Secure Firewall Management Center 用のスタンドアロン Firepower Threat Defense を追加します。スタンドアロン Firepower Threat Defense (FTD) アプリケーションインスタンスを実行する論理デバイスを追加し、Cisco Secure Firewall Management Center (FMC) に登録する必要があります。この論理デバイスは、コンテナインスタンス1 の管理インターフェイスとして機能します。

* 高可用性ペアを追加します。スタンドアロンの FTD アプリケーションインスタンスを実行する別の論理デバイスを追加し、FMC に登録する必要があります。次に、2 つのスタンドアロン FTD 論理デバイス間に高可用性 (HA) を設定する必要があります。これにより、それらに関連付けられているコンテナインスタンスの HA が有効になります1。

最新問題: **190**

ある企業がCisco Secure Endpointプライベートクラウドを導入しています。Secure Endpointプライベートクラウドインスタンスは、サーバ管理者によって既に導入されています。サーバ管理者は、プライベートクラウドインスタンスのホスト名をネットワークエンジニアにメールで提供しました。Cisco Secure Firewall Management CenterからSecure Endpointプライベートクラウドに接続するために、ネットワークエンジニアはサーバ管理者からどのような追加情報を入手する必要がありますか？

A. Secure Endpoint Ornate クラウドインスタンスの SSL 証明書

B. セキュアエンドポイントプライベートクラウドからセキュアエンドポイントパブリッククラウドにアクセスするためのインターネットアクセス

C. Secure Endpoint プライベート クラウド インスタンスのユーザー名とパスワード

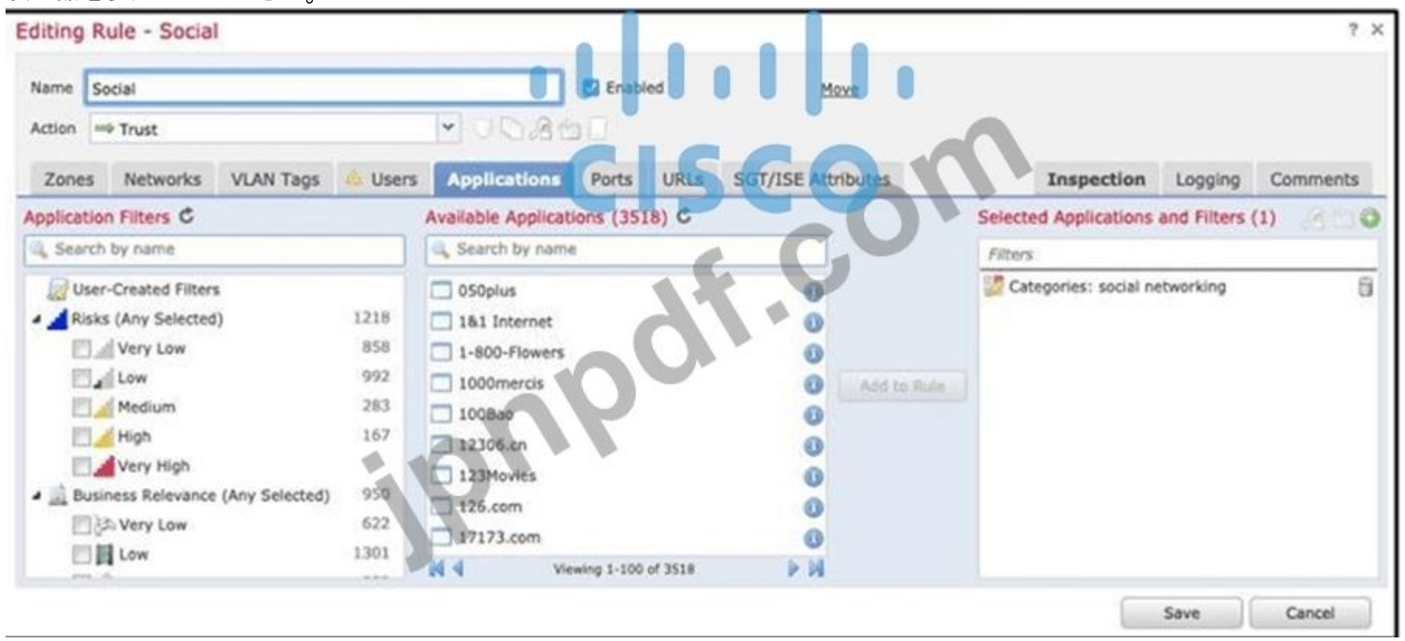
D. 接続プロキシのIPアドレスとポート番号

Answer: (解答を表示する**)**

Cisco Secure Endpoint（旧称AMP for Endpoints）プライベート クラウドを Cisco Secure Firewall Management Center（FMC）と統合する場合、FMC は Secure Endpoint プライベート クラウド インスタンスへの安全な HTTPS 接続を確立する必要があります。

ホスト名は既に提供されていますが、接続設定時の信頼関係の確立にはSSL証明書も必要です。この証明書により、FMCはSecure Endpointプライベートクラウドインスタンスの ID を検証し、通信が暗号化され安全であることを保証できます。

最新問題: **191**
展示品を参照してください。



組織には、すべてのソーシャル メディア トラフィックを検査用に送信することを目的としたアクセス制御ルールがあります。しばらくルールを使用した後、管理者はトラフィックが検査されずに自動的に許可されていることに気付きました。この問題を解決するには、何をする必要がありますか?
A. ルール内で選択したアプリケーションを変更します
B. 侵入ポリシーをセキュリティよりも接続性重視に変更します。
C. ルールアクションを信頼から許可に変更します
D. ソーシャルネットワークのURLをブロックリストに追加する
Answer: A (メーッセージを残す**)**

最新問題: **192**
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部からアクセスできないことに気づきました。ルーティングは正しく設定されているにもかかわらず、リターントラフィックはファイアウォールに入るものの、出てきません。この問題の原因は何でしょうか？
A. NAT テーブルの先頭に手動 NAT 免除ルールが存在しません。
B. 外部 NAT IP アドレスが設定されていません。
C. 外部 NAT IP アドレスが間違ったインターフェースと一致するように設定されています。
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。
Answer: A (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify
最新問題: **193**
FTD ユニットにログインしたときに、ユニットがローカルで管理されているか、リモート FMC サーバーによって管理されているかを判断するために CLI で実行されるコマンドはどれですか。

A. システム生成トラブルシューティング
B. 設定セッションを表示
C. 実行中の設定を表示 | マネージャを含める
D. マネージャーを表示
Answer: D (メーッセージを残す**)**

最新問題**: 194**
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. coredump packet-engine 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
Answer: C (メーッセージを残す**)**
理由 :SNORTエンジンのキャプチャには ｢capture-traffic｣コマンドが使用されます。LINAエンジンのキャプチャには ｢capture｣コマンドを使用します。LINAエンジンはデバイスの実際の物理インターフェースを表すため、｢capture｣が唯一の合理的な選択肢です。参考 :https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10 コマンドは 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 です。

最新問題**: 195**
図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ましたが、サーバーからの応答がありません。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保証するには、どのアクションを実行すればよいですか？

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule,  'Ping' , drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
input-interface: ACCESS41_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f8b7e0 flow (NA)/NA
```

A. 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。
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 署名を設定します。
C. ICMP トラフィックを許可するように Snort ルールを変更します。
D. ICMP 許可リストを作成し、ICMP 宛先を追加して暗黙的な拒否リストから削除します。

Answer: A (メーッセージを残す)
https://community.cisco.com/t5/network-security/ftd-firewall-blocked-or-blacklisted/td-p/4494363

最新問題: **196**
展示を参照してください。エンジニアは、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を搭載したCisco Secure Firewall 9300セキュリティアプライアンス2台
2.0(1.23)
- Cisco Secure Firewall Threat Defense 6.0 1 1 (ビルド 1023) 1 台
- Cisco Secure Firewall Management Center 1台 $W 6 0.1.1ビルド）
1023）
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. 両方のファイアウォールのインターフェース数は同じである必要があります
B. 少なくとも 1 つのファイアウォール インターフェイスで DHCP を構成する必要があります。
C. バージョン番号は同じパッチ番号を持つ必要があります
D. 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
Answer: A (メーッセージを残す)

最新問題: **197**
セキュリティ エンジニアは、複数のブランチ ロケーションに対してアクセス制御ポリシーを構成しています。これらのロケーションは共通のルール セットを共有し、各ロケーションでローカルに重要な内部ネットワーク サブネットを含む INSIDE_NET と呼ばれるネットワーク オブジェクトを使用します。各ロケーションでポリシーの一貫性を維持しながら、適用可能なルール内でローカルに重要なネットワーク サブネットのみを許可するには、どのような手法が考えられますか。
A. INSIDE_NETネットワークオブジェクトとオブジェクトオーバーライドを使用してACPを作成する
B. デバイスごとに一意のACPを作成する
C. ポリシー継承を利用する
D. Cisco Talosから更新される動的ACPを利用する

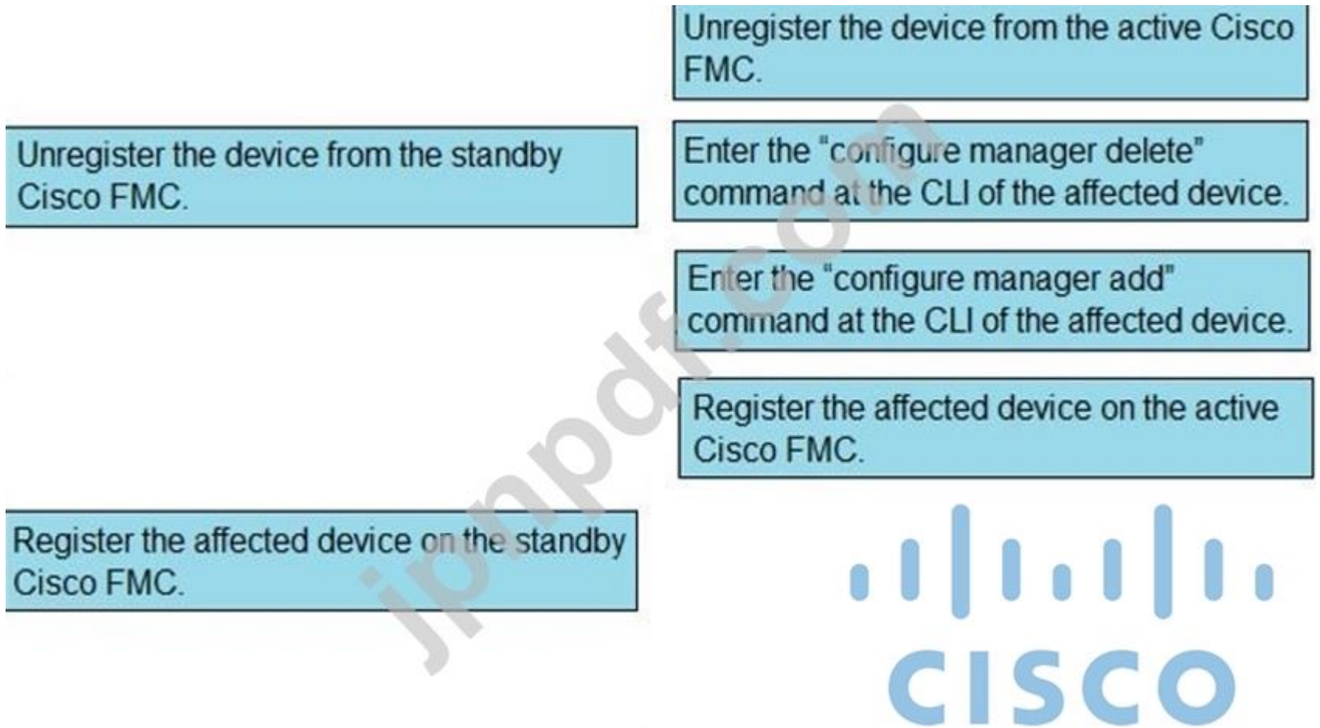
Answer: (解答を表示する**)**

最新問題: **198**
Cisco ASA Firepowerモジュールを導入する際に、組織はネットワークに影響を与えることなくトラフィックの内容を評価したいと考えています。現在、物理アプライアンス上に同一デバイスのインスタンスを複数配置するように設定されています。組織のニーズを満たす導入モードはどれでしょうか？
A. インラインタップモニター専用モード
B. パッシブモニターのみモード
C. パッシブタップモニターのみのモード
D. インラインモード
Answer: A (メーッセージを残す**)**
説明
https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/accessインラインタップモニタ専用モード ASAインライン）インラインタップモニタ専用導入では、トラフィックのコピーがASA FirePOWERモジュールに送信されますが、ASAには返されません。インラインタップモードでは、ネットワークに影響を与えることなく、ASA FirePOWERモジュールがトラフィックに対して行う処理を確認し、トラフィックの内容を評価できます。ただし、このモードではASAはトラフィックにポリシーを適用するため、アクセスルールやTCP正規化などによってトラフィックがドロップされる可能性があります。

最新問題: **199**
ドラッグアンドドロップの質問
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。

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

Answer:



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

最新問題: **200**
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の導入を任されています。各DMZには固有のプライベートIPサブネット範囲があります。この要件はどのように満たされますか？
A. NAT が設定されたルーティング モードでファイアウォールを展開します。
B. NAT が設定された透過モードでファイアウォールを展開します。
C. 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。
D. アクセス制御ポリシーを使用して、ファイアウォールをルーティング モードで展開します。
Answer: D (メーッセージを残す**)**

最新問題: **201**
管理者アクセス権を持つユーザーのみに許可される Cisco Secure Firewall Management Center ウィジェットはどれですか?
A. 製品ライセンス
B. アプライアンス情報
C. システム負荷
D. 現在のセッション
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Management Center の製品ライセンスウィジェットは、管理対象デバイスのライセンス設定など、機密性の高いシステム設定の管理に関係するため、管理者権限を持つユーザー専用です。ライセンス情報の表示と変更に必要な権限は管理者のみに付与されます。
最新問題: **202**

アクセス制御ポリシー内で使用されるオブジェクトを編集した後、どのような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. アクセス制御ポリシーの 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。
Answer: C (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

最新問題**: 203**
エンジニアは LAN スイッチで作業しており、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付きました。トラブルシューティングの結果、スイッチは期待どおりに動作していることが判明しました。この障害が発生するには、何を実装する必要があるのでしょうか。
A. Cisco IPSは検出モードに設定されています
B. Cisco IPSはフェールオープンモードに設定されています
C. 上流ルータのルーティングプロトコルの設定が誤っています
D. リンクステート伝播が有効になっています
Answer: (解答を表示する**)**

最新問題**: 204**
Cisco Firepower NGFW のパッシブ インターフェイスに関する正しい説明はどれですか?
A. NGIPSで指定されたトラフィックを受信します
B. 無効にするとアクセスできなくなります
C. ファイアウォールモードの影響を受けます
D. 受信したトラフィックを再送信します
Answer: A (メーッセージを残す**)**

- Pure IDS deployment–If you do not want to use the system as a firewall or IPS (intrusion prevention system), you can deploy it passively as an IDS (intrusion detection system). In this deployment method, you would use an access control rule to apply an intrusion policy to all traffic. You would also have the system monitor multiple source ports on the switch. Then, you would be able to use the dashboards to monitor the threats seen on the network. However, in this mode, the system can do nothing to prevent these threats.

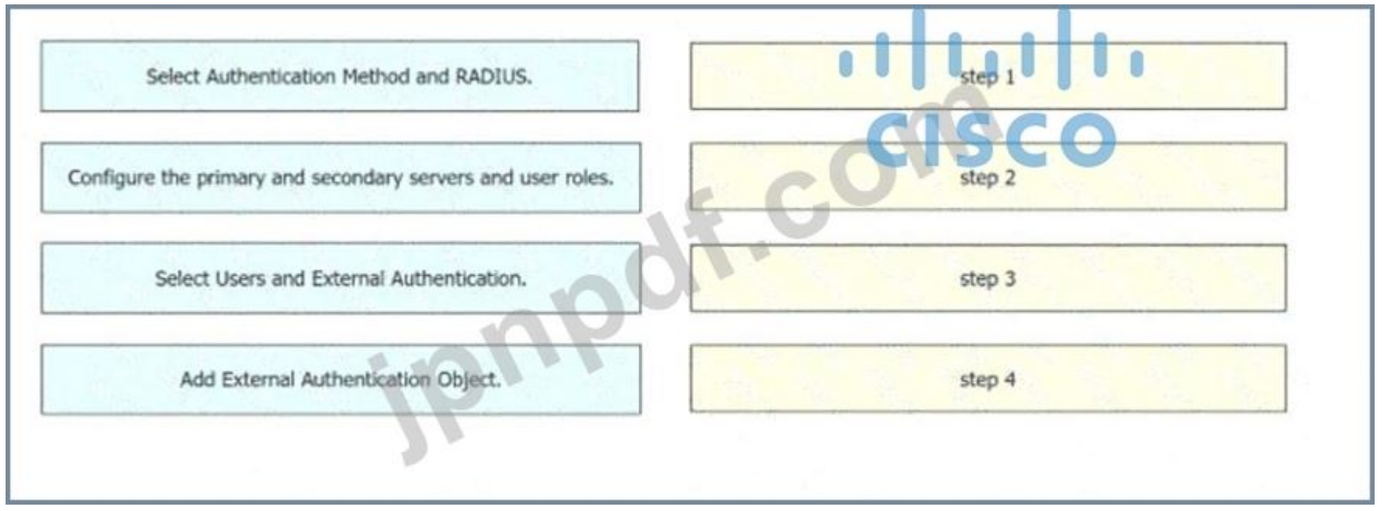
最新問題**: 205**
エンジニアがpxGridを使用してCisco FMCとCisco ISEを統合します。Cisco FMCにはどのようなロールが割り当てられていますか？
A. クライアント
B. サーバー
C. コントローラー
D. 出版社
Answer: A (メーッセージを残す**)**

最新問題**: 206**
QUESTION NO: 95Cisco FMC GUI
を介して Cisco NGFW を初期導入する際に、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. 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。

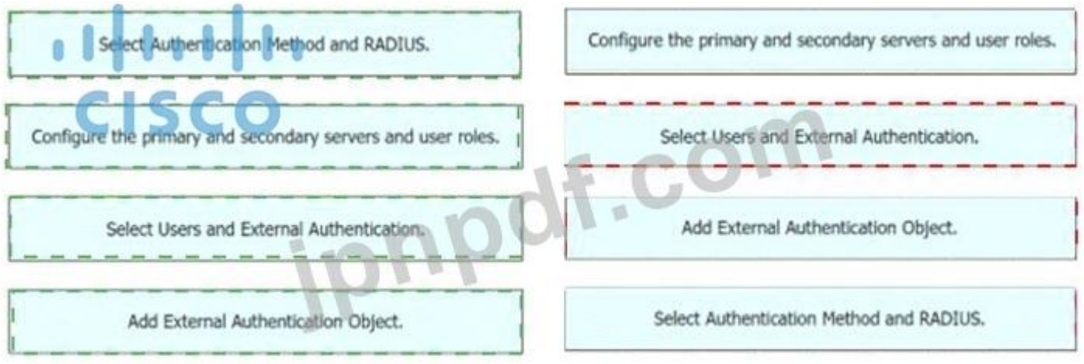
B. IPアドレスを全て拒否
C. ポリシールールは含まれていません
D. IPアドレスを任意に許可
Answer: C (メーッセージを残す**)**
セクション: 展開

最新問題**: 207**
ある企業がIPS機能を備えたCisco Secure Firewall Threat Defenseを導入しています。トラフィックの急増時に検査なしでトラフィックを通過させ、ネットワークトラフィックの安全性を確保するには、インラインモードで何を実装する必要がありますか？
A. インターフェースモードをルーティングに変更します
B. リンク状態の伝播を選択
C. Snortフェイルセーフオプションを設定する
D. MTUを9000に増やす
Answer: (解答を表示する**)**

最新問題**: 208**
左側の設定手順を右側のシーケンスにドラッグ アンド ドロップして、Cisco FMC で RADIUS サーバーへの外部認証を有効にします。



Answer:



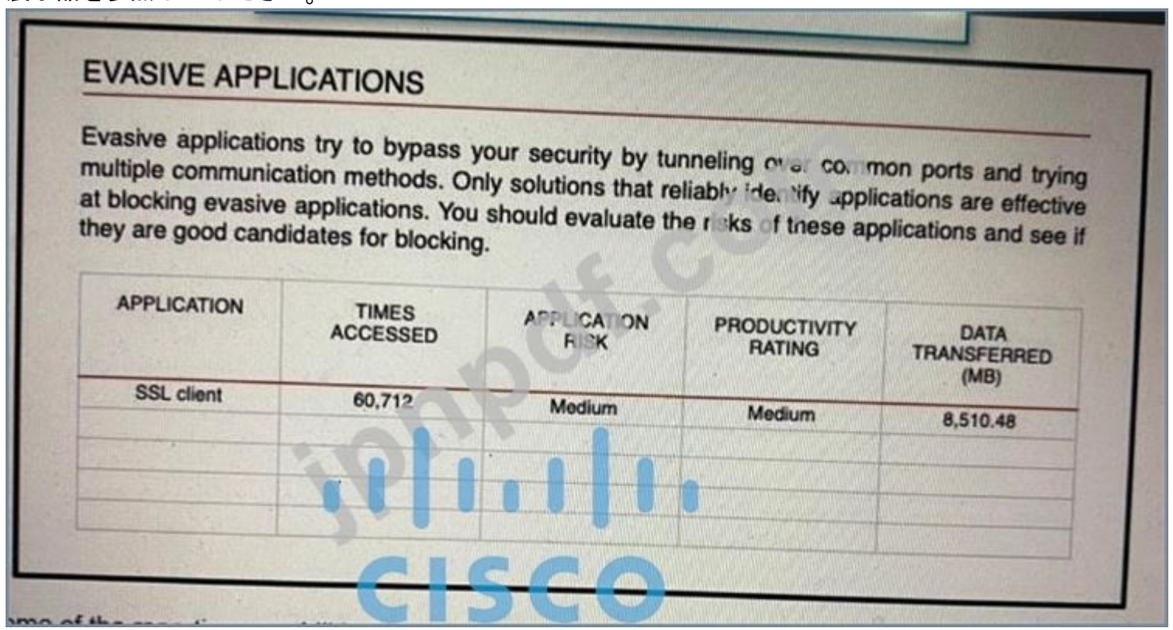
Explanation:
4、1、2、3

最新問題: **209**
ある組織は、Cisco Firepowerデバイスを使用して、ブランチオフィスから本社ビルへのトラフィックを保護したいと考えています。また、Cisco FirepowerデバイスがVPNトラフィックの検査にリソースを浪費しないようにしたいと考えています。これらの要件を満たすには、何をすべきでしょうか？
A. プレフィルタポリシーを使用して、VPNトラフィックを無視するようにCisco Firepowerデバイスを設定します。
B. flexconfigポリシーを有効にしてVPNトラフィックを再分類し、関心のあるトラフィックとして表示されないようにします。
C. VPN トラフィックのアクセス制御ポリシーをバイパスするように Cisco Firepower デバイスを設定します。
D. 侵入ポリシーを調整して、VPNトラフィックが検査なしで通過できるようにします。
Answer: (解答を表示する**)**
説明
Cisco FirepowerデバイスをVPNトラフィックのアクセス制御ポリシーをバイパスするように設定すると、デバイスはVPNトラフィックを検査しないため、リソースを無駄に消費しません。これは、VPNトラフィックがCisco Firepowerデバイスのリソースを無駄に消費しないようにするための最適なオプションです。
参照：
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-c

最新問題: **210**
添付資料を参照してください。エンジニアが、IPSインラインペアモードのSecure Firewall Threat Defenseインターフェイスを使用して、Cisco Secure Firewall Threat Defenseのインスタンスを設定しています。エンジニアはインターフェイスe1/6に何を設定する必要がありますか？

A. フェイルセーフが無効
B. リンク状態の伝播が無効
C. インラインセットMTUを1500に設定
D. セキュリティゾーンが OUTSIDE_ZONE に設定されました
Answer: B (メーッセージを残す**)**
図に示すようにインラインペアモード（e1/6をINSIDE、e1/8をOUTSIDE）を設定する場合、インターフェースで「Propagate Link State」を無効にする必要があります。これにより、一方のリンクがダウンしても、もう一方のインターフェースがダウンすることがなくなり、侵入防御のテストやチューニングにおいて重要となります。

最新問題: **211**
展示品を参照してください。


EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

管理者がCisco Firepowerのレポート機能を確認していたところ、ネットワークリスクレポートのこのセクションに、回避に利用される可能性のあるSSLアクティビティが多数表示されていることに気づきました。このリスクを軽減するには、どのような対策を講じればよいでしょうか？
A. 暗号化されたトラフィック分析を使用して攻撃を検出する
B. SSL 復号化を使用してパケットを分析します。
C. Cisco Tetration を使用して、サーバへの SSL 接続を追跡します。
D. Cisco AMP for Endpoints を使用してすべての SSL 接続をブロックします
Answer: B (メーッセージを残す**)**

最新問題: **212**
組織では、HTTP トラフィックをブロックするときに、デフォルトの Cisco Firepower ブロック ページを使用したくありません。
組織は、ブロックが発生するたびにユーザーを教育するために、ポリシーと手順に関する情報を記載したいと考えています。これらの要件を満たすために必要な2つの手順はどれですか？ 2つ選択してください。）
A. Python を使用して、システム提供のブロック ページの結果を変更します。
B. ポリシーと手順の情報を含む HTML コードを作成します。
C. アクセス制御ポリシーの HTTP 応答をカスタムに変更します。
D. ポリシーと手順の情報を含む CSS コードを記述します。
E. アクセス制御ポリシー内の HTTP 要求処理をカスタマイズされたブロックに編集します。
Answer: (解答を表示する**)**

最新問題: **213**
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ました。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、どのアクション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. キャプチャトラフィックコマンドの一部として詳細オプションを使用します。
C. 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。
D. 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。
Answer: C (メーッセージを残す**)**

最新問題: **214**
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にはどのインターフェイス モードを設定する必要がありますか?
A. インラインセット
B. 受動態
C. ルーティング
D. インラインタップ
Answer: B (メーッセージを残す**)**
参考: 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

最新問題: **215**
Cisco Secure Cloud Analytics はネットワーク トラフィックに関する情報をどのように処理しますか?
A. 情報を分析せずにデータベースに保存します。
B. イベントとネットワーク フロー データに対してヒューリスティック分析を実行します。
C. 情報を保存せずに他のデバイスに転送します。
D. イベントおよびネットワーク フロー データの動作分析を実行します。
Answer: D (メーッセージを残す**)**
Cisco Secure Cloud Analytics（旧称Stealthwatch Cloud）は、行動分析を用いてイベントとネットワークフローデータを監視します。正常なネットワーク行動のベースラインを構築し、データ漏洩やラテラルムーブメントといった潜在的な脅威を示唆する異常を検出します。

最新問題: **216**
ネットワーク管理者は、レイヤ7インスペクションを回避するために、Cisco Firepowerでトラフィックを高速パスするポリシーを作成する必要があります。トラフィックのインスペクションレートを最適化する必

要があります。この目標を達成するには、何をすべきでしょうか？
A. マルチインスタンス用に FXOS を有効にします。
B. プレフィルタ ポリシーを構成します。
C. モジュラー ポリシー フレームワークを構成します。
D. TCP 検査を無効にします。
Answer: B (メーッセージを残す)
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/prefiltering_and_prefilter_policies.html

最新問題**: 217**
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. Cisco セキュア ファイアウォール VDC
B. Cisco ISE コンテキスト
C. TACACS+デー タベース
D. AD定義
Answer: D (メーッセージを残す)
Cisco Identity Services Engine（ISE）とCisco Firewall Management Center（FMC）の統合では、Active Directory（AD）設定を定義するためにレルムが使用されます。FMCのレルムは、ユーザーの認証と承認に必要なADサーバ、ドメイン、その他の認証設定を指定します。
レルムを構成する手順:
FMC で、[システム] > [統合] > [レルムとディレクトリ] に移動します。
新しい領域を追加し、AD 設定を構成します。
シームレスな統合を実現するために、レルム設定がAD環境と一致していることを確認してください。レルムはADとFMCの統合に不可欠であり、ファイアウォールがユーザー認証とポリシー適用にADを使用できるようにします。

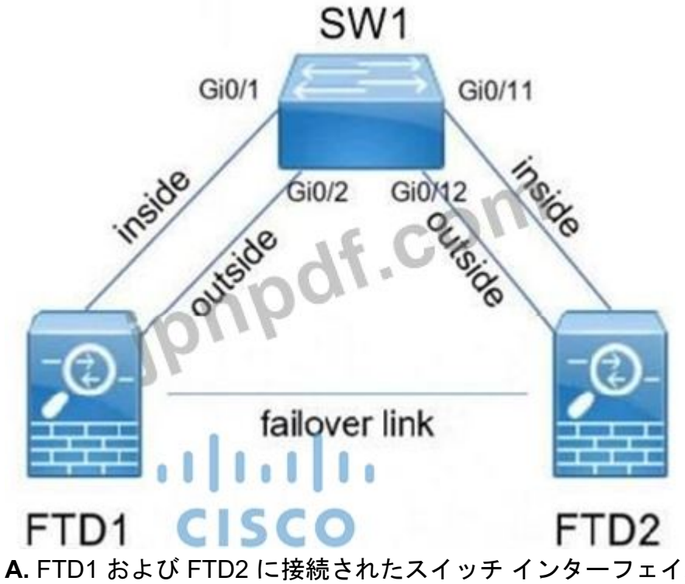
最新問題**: 218**
エンジニアが新しいCisco Secure Firewallを実装しています。このファイアウォールは、以下の3つのサブネット間のトラフィックをフィルタリングする必要があります。
- LAN 192.168.101.0/24
- DMZ 192.168.200.0/24
- WAN 10.0.0.0/30
エンジニアはどのファイアウォール モードを実装する必要がありますか?
A. 透明
B. ネットワーク
C. ルーティング
D. ゲートウェイ
Answer: C (メーッセージを残す)
複数のサブネット間のトラフィックをフィルタリングするには、エンジニアはファイアウォールをルーテッドモードで実装する必要があります。ルーテッドモードでは、ファイアウォールはレイヤ3デバイスとして動作し、異なるIPサブネット間のトラフィックをルーティングできます。このモードは、LAN、DMZ、およびWANサブネット間のトラフィックのフィルタリングに適しています。
ルーティング モードを設定する手順:
ファイアウォールの管理インターフェイスにアクセスします。
適切な IP アドレスとネットワーク マスクを使用して、各サブネット (LAN、DMZ、WAN) のインターフェイスを構成します。
セキュリティ ゾーンを定義し、アクセス制御ポリシーを適用して、必要に応じてトラフィックをフィルターします。

これにより、ファイアウォールは異なるサブネット間のトラフィックを検査およびルーティングできるようになり、必要なセキュリティと制御が提供されます。

最新問題: **219**
エンジニアはネットワークにCisco FTDを実装しており、どのFirepowerモードを使用するかを検討しています。組織では、トラフィックセグメンテーションを実現するために、FTDアプライアンス内で個別に動作する複数の仮想Firepowerデバイスが必要です。これらの要件を満たすには、Cisco Firepower管理コンソールでどの導入モードを設定する必要がありますか？
A. マルチインスタンス
B. シングルコンテキスト
C. 複数の展開
D. 単一のデプロイメント
Answer: A (メーッセージを残す**)**

最新問題: **220**
図を参照してください。ある企業では、FTD1とFTD2という名のCisco Secure Firewall Threat Defenseデバイスのペアを導入しています。FTD1とFTD2は、フェイルオーバーリンクはありますがステートフルリンクのないアクティブ/スタンバイペアとして設定されています。FTD1に障害が発生した場合でも、社内ネットワークのユーザーが外部デバイスと通信できるようにするには、次に何を実装する必要がありますか？

```
Gi0/1 and Gi0/11 configuration:
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown

Gi0/2 and Gi0/12 configuration:
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
```



A. FTD1 および FTD2 に接続されたスイッチ インターフェイスのポート セキュリティを無効にします。
B. FTD1 および FTD2 のスイッチ インターフェイスで、最大保護アドレスを 2 に設定します。

C. ステートフル リンクを接続して構成し、変更を展開します。
D. SW1 および FTD2 でスパニングツリー PortFasl 機能を設定します。
Answer: C (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスを使用したフェイルオーバー構成では、プライマリデバイス（FTD1）に障害が発生した場合でも、内部ネットワーク上のユーザが外部デバイスとの通信を継続できるようにするため、ステートフルフェイルオーバーリンクを実装する必要があります。ステートフルフェイルオーバーリンクにより、セカンダリデバイス（FTD2）はセッション情報と状態データを維持できるため、シームレスなフェイルオーバーが実現し、中断を最小限に抑えることができます。
ステートフル フェイルオーバー リンクを実装する手順:
FTD1 と FTD2 の間にステートフル フェールオーバー リンクを物理的に接続します。
FMC でステートフル フェールオーバー リンクを設定します。
両方のデバイスが適切に同期され、ステートフル フェイルオーバーが有効になっていることを確認します。
両方の FTD デバイスに変更を展開します。
ステートフル リンクを設定すると、セカンダリ FTD は、ユーザーが接続を再確立する必要なくアクティブなセッションを引き継ぐことができるため、継続的な通信が保証されます。

最新問題**: 221**
Firepower をしばらく使用し、ネットワークとのやり取り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とユーザーを関連付けようとしています。Cisco Firepower ダッシュボードでこの可視性を実現するには、どのウィジェットを設定する必要がありますか?
A. 現在のステータス
B. 相関イベント
C. カスタム分析
D. 現在のセッション
Answer: B (メーッセージを残す**)**

最新問題**: 222**
エンジニアは、Cisco FTDでパケットキャプチャを実行し、IPアドレス192を使用しているホストが
168.100.100 の MAC アドレスは 0042 7734.103 で、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 送信元 192.168.100.100
B. -src 192.168.100.100 なし
C. -w キャプチャ.pcap -s 1518 ホスト 192.168.100.100 mac
D. -w capture.pcap -s 1518 ホスト 192.168.100.100 イーサ
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-def

最新問題**: 223**
エンジニアはネットワークに冗長性を構築し、ファイアウォールの手前にある冗長スイッチがダウンした場合でもトラフィックが途切れることなく流れるようにする必要があります。このタスクを実現するには、どのような設定が必要ですか？
A. ファイアウォール クラスタ モードおよびスイッチ上の冗長インターフェイス
B. ファイアウォール非クラスタモードおよびスイッチ上の冗長インターフェース
C. スイッチ上のvPCをファイアウォールダスターのインターフェースモードにする

D. スイッチ上のvPCからファイアウォールクラスタ上のSPAN EtherChannelへ
Answer: D (メーッセージを残す**)**
参考: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf

最新問題**: 224**
ある企業がCisco Secure Endpointプライベートクラウドを導入しています。Secure Endpointプライベートクラウドインスタンスは、サーバ管理者によって既に導入されています。サーバ管理者は、プライベートクラウドインスタンスのホスト名をネットワークエンジニアにメールで提供しました。Cisco Secure Firewall Management CenterからSecure Endpointプライベートクラウドに接続するために、ネットワークエンジニアはサーバ管理者からどのような追加情報を入手する必要がありますか？
A. Secure Endpoint Ornate クラウドインスタンスの SSL 証明書
B. セキュアエンドポイントプライベートクラウドからセキュアエンドポイントパブリッククラウドにアクセスするためのインターネットアクセス
C. Secure Endpoint プライベート クラウド インスタンスのユーザー名とパスワード
D. 接続プロキシのIPアドレスとポート番号
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Management Center（FMC）からSecure Endpointプライベートクラウドインスタンスに接続するには、ネットワークエンジニアはSecure Endpointプライベートクラウドインスタンス用のSSL証明書が必要です。このSSL証明書は、FMCとプライベートクラウドインスタンス間の安全で信頼できる接続を確立するために不可欠です。
手順:
* サーバー管理者から SSL 証明書を取得します。
* SSL 証明書を FMC にインポートします。
* 提供されたホスト名と SSL 証明書を使用して、Secure Endpoint プライベート クラウド インスタンスへの接続を構成します。
これにより、プライベート クラウド インスタンスへの安全で認証された接続が保証されます。
参考資料: Cisco Secure Firewall Management Center 統合ガイド、セキュア エンドポイント統合の章。

最新問題**: 225**
ある組織は、現時点では悪評が知られていない Web サイトからマルウェアがダウンロードされたことに気付きました。
この問題は、どのようにすれば世界的に、可能な限り迅速に、そして最小限の影響で解決されるのでしょうか?
A. アウトバウンドWebアクセスを拒否する
B. エンドポイントを分離することで
C. Cisco Talos はポリシーを自動的に更新します。
D. ポリシーにURLオブジェクトを作成してウェブサイトをブロックする
Answer: D (メーッセージを残す**)**

最新問題**: 226**
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部からアクセスできないことに気付きました。ルーティングは正しく設定されているものの、戻りトラフィックはファイアウォールには入っているものの、ファイアウォールから出ていない状態です。
この問題の原因は何ですか?
A. NAT テーブルの先頭に手動 NAT 免除ルールが存在しません。
B. 外部 NAT IP アドレスが設定されていません。
C. 外部 NAT IP アドレスが間違ったインターフェースと一致するように設定されています。
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。
Answer: A (メーッセージを残す**)**

NAT 免除は、自動/オブジェクト NAT の前に手動ルールでのみ実行できます。
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

最新問題: **227**
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ポリシーを設定しました。また、すべてのソースがポート80でパブリックIPアドレスにアクセスできるようにするアクセスポリシーも作成しました。しかし、インターネットからポート80を経由してWebサーバーにアクセスできません。どのような設定変更が必要ですか？
A. 送信元 IP アドレスと宛先 IP アドレスを変換するように NAT ポリシーを変更する必要があります。
B. アクション信頼に対してアクセス ポリシー ルールを構成する必要があります。
C. ポート 80 の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。
Answer: D (メーッセージを残す**)**

最新問題: **228**
悪意のあるイベントの増加に伴い、セキュリティエンジニアは侵入イベント、マルウェアイベント、セキュリティインテリジェンスイベントを含む脅威レポートを作成する必要があります。これらの情報はどのようにして単一のレポートに収集されるのでしょうか？
A. デフォルトの Firepower レポートを実行します。
B. カスタム レポートを作成します。
C. マルウェア レポートを生成します。
D. 攻撃リスクレポートをエクスポートします。
Answer: B (メーッセージを残す**)**

最新問題: **229**
ある企業では、Cisco FMCで管理されている多数のCisco FTDデバイスを運用しています。セキュリティモデルでは、分析のためにアクセス制御ルールのログを収集する必要があります。セキュリティエンジニアは、生成されるログの量をCisco FMCが処理できないのではないかと懸念しています。この懸念に対処するには、どのような構成が適切でしょうか？
A. Cisco FTD 接続イベントとセキュリティ イベントを SIEM システムに直接送信し、保存および分析します。
B. Cisco FTD 接続イベントとセキュリティ イベントを Cisco FMC に送信し、ログを SIEM に転送して保存および分析するように設定します。
C. Cisco FTD 接続イベントとセキュリティ イベントを Cisco FMC デバイスのクラスタに送信し、保存および分析します。
D. Cisco FTD 接続イベントを SIEM システムに直接送信し、セキュリティ イベントを Cisco FMC から SIEM システムに転送して保存および分析します。
Answer: (解答を表示する**)**

最新問題: **230**
ネットワーク セキュリティ エンジニアは、高可用性ペア内の障害のある Cisco FTD デバイスを交換する必要があります。
故障したユニットを交換する際には、どのようなアクションを実行する必要がありますか?
A. 障害のあるCisco FTDデバイスをCisco FMCから登録解除します。

B. 交換ユニットの電源を入れる前にCisco FMCをシャットダウンしてください
C. 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。
D. 交換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。
Answer: A (メーッセージを残す**)**

最新問題**: 231**
管理者は、ポリシー内で使用するために、Cisco FMCに新しいURLベースのカテゴリフィードを追加しようとしています。インテリジェンスソースはSTIXではなく、.txtファイル形式を使用しています。定期的な更新を確実に提供するために、どのようなアクションを実行すればよいでしょうか。
A. TAXII フィード ソースを追加し、フィードの URL を入力します。
B. .txt ファイルを STIX に変換し、Cisco FMC にアップロードします。
C. URL ソースを追加し、Cisco FMC 内でフラット ファイル タイプを選択します。
D. .txt ファイルをアップロードし、埋め込まれた URL を使用して自動更新を構成します。
Answer: (解答を表示する**)**

最新問題**: 232**
Cisco Secure Firewall デバイスで IRB モードの分離ブリッジ 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。
Answer: B (メーッセージを残す**)**
Cisco Secure Firewall デバイスで Integrated Routing and Bridging（IRB）モードの分離ブリッジグループを設定するには、BVI（ブリッジ仮想インターフェイス）インターフェイス名を空のままにしておきます。これにより、ブリッジグループは分離された状態で動作し、ブリッジされたインターフェイスにはレイヤ3ルーティングが適用されないため、ブリッジグループ内のトラフィックが効果的に分離されます。
手順:
ファイアウォールの構成インターフェイスにアクセスします。
ブリッジ グループ インターフェイスを設定します。
ブリッジ グループを分離するには、BVI インターフェイス名が空のままになっていることを確認します。
この設定により、分離されたブリッジ グループのレイヤ 3 ルーティングが防止され、トラフィックがブリッジ グループ内に留まるようになります。

最新問題**: 233**
管理者は SNORT 検査ポリシーを設定していますが、Cisco FMC で展開失敗メッセージが表示されます。
トラブルシューティングを支援するために、管理者は Cisco TAC にどのような情報を生成する必要がありますか?
A. 問題のあるデバイスの「トラブルシューティング」ファイル。
B. 問題のデバイスの「show tech」ファイル
C. Cisco FMC の「show tech」。
D. Cisco FMCの「トラブルシューティング」ファイル
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

最新問題**: 234**

アクセス制御ポリシー ルールで使用できる 2 つのアクションはどれですか (2 つ選択してください)。
A. リセット付きブロック
B. モニター
C. 分析
D. 発見
E. すべてをブロック
Answer: A,B (メーッセージを残す**)**
セクション: 構成
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

最新問題**: 235**
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-force-reset
C. システム サポート ssl-client-hello-display
D. システム サポート ssl-client-hello-reset
Answer: D (メーッセージを残す**)**

最新問題**: 236**
管理者は、標準営業時間外に内部ホストから10MBを超えるデータ転送が開始された場合に通知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. ファイルとマルウェアのポリシー
B. アプリケーション検出器
C. 侵入ポリシー
D. 相関ポリシー
Answer: (解答を表示する**)**
相関ポリシーを使用すると、時刻、ユーザー、送信元/宛先IPアドレスなど、さまざまな基準に基づいてセキュリティイベントを相関させることができます。指定された基準が満たされた場合、相関ポリシーはメール通知の送信などのレスポンスアクションをトリガーできます。

最新問題**: 237**
Cisco Firepower システムでは、アクセス制御ポリシーはどのような 2 つの方法で動作しますか? (2 つ選択してください。)
A. 構成の変更が展開されると、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、その後に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. システムは信頼できるトラフィックに対して予備検査を実行し、信頼できるパラメータと一致するかどうかを検証します。
E. ファイル ポリシーは、関連付けられた変数セットを使用して侵入防止を実行します。
Answer: A,C (メーッセージを残す**)**

最新問題**: 238**
エンジニアは、最近追加された新しいサーバが、現在ファイアウォールによって分離されている既存のサーバと通信する必要があるため、Cisco Secure Firewall の透過モードを実装する必要があります。この目標を達成するために、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. 両方のサーバーに同じサブネットを割り当てます。
C. 両方のサーバーが同じブリッジ ドメイン内にあることを確認します。
D. 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。
Answer: C (メーッセージを残す**)**

最新問題: **239**
エンジニアは、Cisco FTD侵入ポリシーにDNS固有のルールを追加する必要があります。エンジニアは、Cisco FTD Snortデータベースで現在有効になっていないルールを使用したいと考えていますが、必要以上に有効にしたくはありません。これらの要件を満たすアクションはどれですか？
A. 推奨事項の生成と使用機能を使用してルールを変更します。
B. 基本ポリシーを 接続性よりもセキュリティを優先」に変更します。
C. ポリシー内のルールの動的な状態を変更します。
D. 使用中のポリシー内のルールの状態を変更します。
Answer: D (メーッセージを残す**)**

最新問題: **240**
Cisco Firepower NGIPS のネットワーク分析ポリシーの目的は何ですか?
A. 高度な検査を使用せずにトラフィックを処理するために使用される外部ヘッダー基準を指定します。
B. 検査前にトラフィックを前処理する方法を制御します
C. トラフィックを暗号化するためのルールを定義します
D. 侵入ルールを使用してパケットの攻撃を検査します
Answer: B (メーッセージを残す**)**

最新問題: **241**
IT管理者は、ネットワークエンジニアに対し、ネットワーク内のCisco FTDアプライアンスの高レベルな概要統計情報を提供するよう依頼しています。ビジネスはピークシーズンに近づいており、ビジネスの稼働時間を維持する必要性が高まっています。この情報を収集するには、どのレポートタイプを使用すればよいでしょうか？
A. マルウェアレポート
B. リスクレポート
C. SNMPレポート
D. 標準レポート
Answer: B (メーッセージを残す**)**

最新問題: **242**
ソフトウェア開発会社は、請負業者が社内開発者と共同で取り組んでいるプロジェクトのコードを共有するためのウェブサイト http:dev.company.com をホストしています。このウェブサーバはオンプレミスで、Cisco Secure Firewall Threat Defense アプライアンスによって保護されています。ネットワーク管理者は、このサイト経由で感染ファイルを社内ユーザーに送信しようとする人物がいるのではないかと懸念しています。Cisco Secure Firewall Malware Defense がマルウェアを検出 ･ブロックするには、アクセス制御ポリシーにどのタイプのポリシーを関連付ける必要がありますか？
A. SSLポリシー

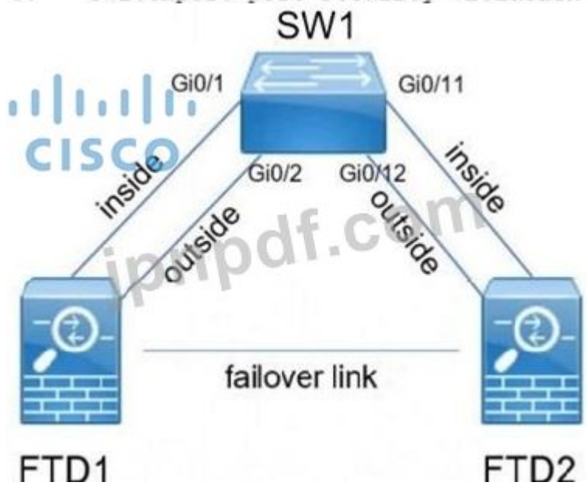
B. プレフィルターポリシー
C. ファイルポリシー
D. ネットワーク検出ポリシー
Answer: C (メーッセージを残す**)**
Cisco Secure Firewall Malware Defense がマルウェアを検出してブロックできるようにするには、ネットワーク管理者がファイルポリシーをアクセス制御ポリシーに関連付ける必要があります。ファイルポリシーにより、管理者は Cisco Secure Firewall Threat Defense アプライアンス上でマルウェア検出およびファイル分析機能を設定できます。
ファイル ポリシーを構成する手順:
* FMC で [ポリシー] > [アクセス制御] > [ファイル ポリシー] に移動します。
* 新しいファイル ポリシーを作成するか、既存のファイル ポリシーを編集して、マルウェアの検出とブロックの設定を含めます。
* ファイル ポリシーを関連するアクセス制御ポリシーに関連付けます。
* アクセス制御ポリシーが FTD アプライアンスに展開されていることを確認します。
ファイル ポリシーを関連付けると、ファイアウォールは Web サーバーを介して送信されるファイルにマルウェアが含まれていないか検査し、構成されたルールに基づいて適切なアクション (ブロック、許可、または警告) を実行します。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、ファイル ポリシーの章。

最新問題: **243**
エンジニアは新しい Firepower の展開を設定しており、実装を開始するためにデフォルトの FMC ポリシーを確認しています。組織は、最初の試用フェーズで、ネットワーク トラフィックの大部分を通過させながら、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。どのデフォルト ポリシーを使用する必要がありますか。
A. 最大検出
B. 接続性よりもセキュリティを重視
C. バランスの取れたセキュリティと接続性
D. セキュリティよりも接続性を重視
Answer: (解答を表示する)
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusio

最新問題: **244**
エンジニアがセキュリティゾーンまたはトンネルゾーンにファイルポリシー設定を展開するアクセス制御ルールを設定したところ、デバイスが再起動しました。再起動の理由は何ですか？
A. アクセス制御ルール内の送信元または宛先のセキュリティ ゾーンは、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致します。
B. ルール内のソース トンネル ゾーンが、宛先ポリシー内のトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
C. ソース トンネル ゾーン内のソースまたは宛先セキュリティ ゾーンが、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致しません。
D. ルール内のソース トンネル ゾーンが、ソース ポリシー内のトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
Answer: A (メーッセージを残す**)**
これらのファイル ポリシー構成をセキュリティ ゾーンまたはトンネル ゾーンに展開するアクセス制御ルールでは、構成が次の条件を満たしている場合にのみ再起動が発生することに注意してください。
アクセス制御ルール内の送信元または宛先のセキュリティ ゾーンは、ターゲット デバイスのインターフェイスに関連付けられたセキュリティ ゾーンと一致する必要があります。
アクセス制御ルール内の宛先ゾーンが any でない限り、ルール内の送信元トンネル ゾーンは、プレフィルタ ポリシー内のトンネル ルールに割り当てられたトンネル ゾーンと一致する必要があります。
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/policy_management.html

最新問題: **245**
図を参照してください。ある企業では、FTD1とFTD2という名のCisco Secure Firewall Threat Defenseデバイスのペアを導入しています。FTD1とFTD2は、フェイルオーバーリンクはありますがステートフルリンクのないアクティブ/スタンバイペアとして設定されています。FTD1に障害が発生した場合でも、社内ネットワークのユーザーが外部デバイスと通信できるようにするには、次に何を実装する必要がありますか？

```
Gi0/1 and Gi0/11 configuration:
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown

Gi0/2 and Gi0/12 configuration:
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
```



A. FTD1 および FTD2 に接続されたスイッチ インターフェイスのポート セキュリティを無効にします。
B. FTD1 および FTD2 のスイッチ インターフェイスで、最大保護アドレスを 2 に設定します。
C. ステートフル リンクを接続して構成し、変更を展開します。
D. SW1 および FTD2 でスパニングツリー PortFasl 機能を設定します。
Answer: C (メーッセージを残す)
Cisco Secure Firewall Threat Defense（FTD）デバイスを使用したフェイルオーバー構成では、プライマリデバイス（FTD1）に障害が発生した場合でも、内部ネットワーク上のユーザが外部デバイスとの通信を継続できるようにするため、ステートフルフェイルオーバーリンクを実装する必要があります。ステートフルフェイルオーバーリンクにより、セカンダリデバイス（FTD2）はセッション情報と状態データを維持できるため、シームレスなフェイルオーバーが実現し、中断を最小限に抑えることができます。
ステートフル フェイルオーバー リンクを実装する手順:
FTD1 と FTD2 の間にステートフル フェールオーバー リンクを物理的に接続します。
FMC でステートフル フェールオーバー リンクを設定します。
両方のデバイスが適切に同期され、ステートフル フェイルオーバーが有効になっていることを確認します。
両方の FTD デバイスに変更を展開します。
ステートフル リンクを設定すると、セカンダリ FTD は、ユーザーが接続を再確立する必要なくアクティブなセッションを引き継ぐことができるため、継続的な通信が保証されます。

最新問題: **246**
アクセス制御ポリシー ルールで使用できる 2 つのアクションはどれですか (2 つ選択してください)。
A. リセット付きブロック

B. モニター
C. 分析
D. 発見
E. すべてをブロック
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

最新問題**: 247**
高可用性の実行を一時的に停止するには、プライマリ Cisco FTD ユニットの CLI でどのコマンドを入力しますか?
A. 高可用性再開を構成する
B. 高可用性を無効にする
C. システムサポートネットワークオプション
D. 高可用性サスペンドを構成する
Answer: B (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html

最新問題**: 248**
展示品を参照してください。

エンジニアがCisco Secure Firewall Management Center（FMC）でトラブルシューティングファイルを生成します。ファイルがダウンロードされる前に、正常に完了したタスクが削除されます。ファイル名を特定し、生成されたトラブルシューティングファイルを再生成せずに取得するには、どの2つの操作を実行する必要がありますか？ 2つ選択してください。）
A. Secure FMC の FTP クライアント Hi エキスパート モードを使用して、ファイルを FTP サーバーにアップロードします。
B. 図に示されているのと同じ画面に移動し、 高度なトラブルシューティング」をクリックし、ファイル名を入力してダウンロードを開始します。
C. FTD67 および FTD66 デバイスの CU に接続し、フラッシュから PIP サーバーにタイルをコピーします。
D. Secure FMCのエキスパートモードに移行します。/Var/commonの内容を一覧表示し、出力から正しいファイル名を決定します。
E. [システム監視]、[監査] の順にクリックし、[トラブルシューティング ファイルの生成] 文字列を含む行から正しいファイル名を決定します。
Answer: D,E (メーッセージを残す**)**
Cisco Secure Firewall Management Center (FMC) でトラブルシューティング ファイルを生成するタスクが正常に完了したが、ファイルがダウンロードされる前に削除された場合は、次の手順を実行してファイル名を決定し、生成されたトラブルシューティング ファイルを再生成せずに取得できます。
* Secure FMC のエキスパート モードに移動します。
* SSH またはコンソール経由で FMC のエキスパート モードにアクセスします。
* 生成されたトラブルシューティングファイルを見つけるには、/var/commonディレクトリの内容を一覧表示します。ls /var/commonコマンドを使用してください。

* システム監視監査ログを使用します。
* FMC で、[システム] > [監視] > [監査] に移動します。
* 「Generate Troubleshooting Files」という文字列を含む行を見つけて、正しいファイル名を確認します。
これらのアクションにより、生成されたトラブルシューティング ファイルを再生成する必要なく識別して取得できるため、時間とリソースを節約できます。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、トラブルシューティングとファイル管理の章。

最新問題: **249**
2 つの Cisco FTD デバイス間で高可用性を実現するには、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設定
C. 同じDHCP/PPoE設定
D. 同じホスト名
E. インターフェースの数が同じ
Answer: B,E (メーッセージを残す**)**
説明
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-aConditions 2 台の FTD デバイス間に HA を作成するには、次の条件を満たす必要があります。
同じモデル
同じバージョン（これは FXOS と FTD に適用されます - メジャー（最初の番号）、マイナー（2 番目の番号）、メンテナンス（3 番目の番号）は同じである必要があります）（同数のインターフェイス、同じタイプのインターフェイス、両方のデバイスが FMC 内の同じグループ/ドメインの一部である、同一のネットワーク タイム プロトコル（NTP）設定がある、コミットされていない変更なしで FMC に完全に展開されている、同じファイアウォール モード（ルーテッドまたはトランスペアレント）である。
FTD が同じモードであっても、FMC がこれを反映しないケースがあるため、FTD デバイスと FMC GUI の両方でこれを確認する必要があることに注意してください。
いずれのインターフェースにもDHCP/Point-to-Point Protocol over Ethernet（PPPoE）が設定されていません。両方のシャーシで異なるホスト名（完全修飾ドメイン名（FQDN）が設定されています。シャーシのホスト名を確認するには、FTD CLIにアクセスし、次のコマンドを実行します。

最新問題: **250**
ネットワーク管理者は、デバイスのすべての非管理インターフェースで検査が中断されていることに気づきました。原因は何でしょうか？
A. 管理以外のインターフェースに割り当てられた最高 MTU の値が変更されました。
B. 管理以外のインターフェースに割り当てられた最高 MSS の値が変更されました。
C. 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ました。
D. 同じインライン インターフェイスに複数のインライン インターフェイス ペアが追加されました。
Answer: A (メーッセージを残す**)**
デバイス上のすべての非管理インターフェースの中で最大のMTU値を変更すると、設定変更の適用時にSnortプロセスが再起動され、トラフィックの検査が一時的に中断されます。検査は、変更したインターフェースだけでなく、すべての非管理インターフェースで中断されます。この中断によってトラフィックがドロップされるか、それ以上の検査を行わずに通過するかは、管理対象デバイスのモデルとインターフェースの種類によって異なります。詳細については、「Snort® の再起動によるトラフィックの動作」を参照してください。
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01101010.html

最新問題: **251**
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透過的な Cisco FTD デバイスを設定していますが、FTD がトラフィックを処理していません。問題は何でしょうか。
A. 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。
B. スイッチは、FTDで定義されたフローIDと一致するモニターセッションIDで設定されていません。

C. 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。
D. ERSPAN トラフィックを処理するには、FTD をルーティング モードにする必要があります。
Answer: D (メーッセージを残す**)**

最新問題**: 252**
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。エンジニアが次のURLにアクセスした場合：
https:///capture/CAPI/pcap/sample.pcap
エンジニアはPCAPファイルが提供されず、403: Forbiddenエラーを受け取りました。この問題を解決するには、どのような操作が必要ですか？
A. クライアント ブラウザーのプロキシ設定を無効にします。
B. HTTPS サーバーを無効にして、HTTP を使用します。
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. 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。
Answer: C (メーッセージを残す**)**
403: Forbiddenエラーは、Secure Firewall Threat Defense（FTD）デバイス上のHTTPSサーバが適切に設定または有効化されていないため、要求されたPCAPファイルにアクセスできないことを示しています。この問題を解決するには、エンジニアはCisco Secure Firewall Management Center（FMC）でFTDデバイスに適用されているデバイスプラットフォームポリシーでHTTPSサービスを有効にする必要があります。これにより、FTDはPCAPファイルへのアクセスを含むHTTPSリクエストを処理できるようになります。

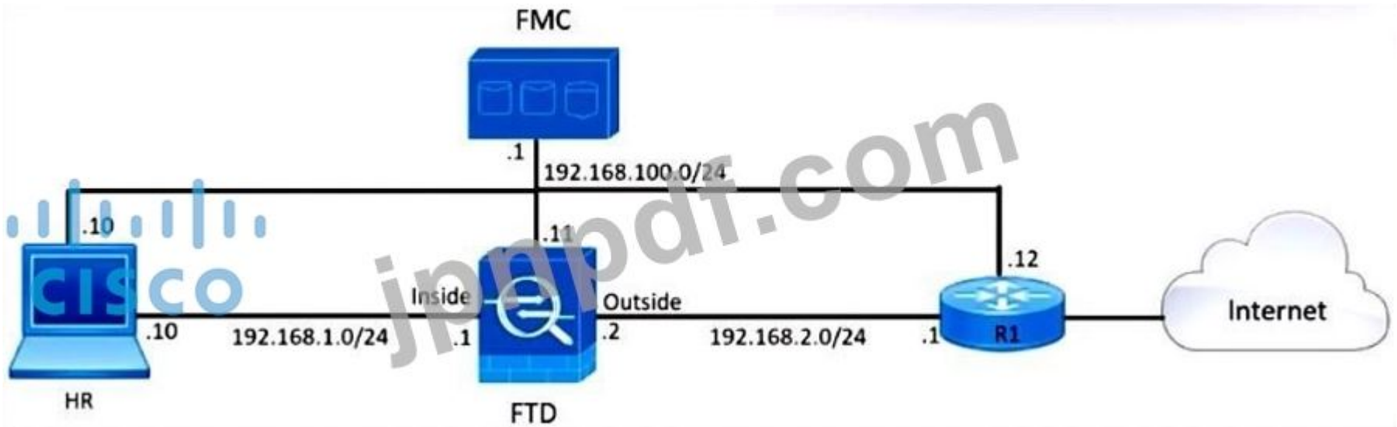
最新問題**: 253**
ネットワークエンジニアは、Cisco Secure Firewall Threat Defenseアプライアンスとネットワーク間のケーブル配線を設定する必要があります。これにより、Secure Firewall Threat Defenseアプライアンスは、生成された侵入イベントをインラインで分析および調整し、本番稼働前にその処理を実行する必要があります。エンジニアはどのSecure Firewall Threat Defenseインターフェイスモードを使用する必要がありますか？
A. リンク状態の伝播
B. バイパス
C. 厳密なTCP強制
D. タップモード
Answer: (解答を表示する**)**

最新問題**: 254**
ある組織は、Cisco Firepowerデバイスを使用して、ブランチオフィスから本社ビルへのトラフィックを保護したいと考えています。また、Cisco FirepowerデバイスがVPNトラフィックの検査にリソースを浪費しないようにしたいと考えています。これらの要件を満たすには、何をすべきでしょうか？
A. プレフィルタポリシーを使用して、VPNトラフィックを無視するようにCisco Firepowerデバイスを設定します。
B. flexconfigポリシーを有効にしてVPNトラフィックを再分類し、関心のあるトラフィックとして表示されないようにします。
C. VPN トラフィックのアクセス制御ポリシーをバイパスするように Cisco Firepower デバイスを設定します。
D. 侵入ポリシーを調整して、VPNトラフィックが検査なしで通過できるようにします。
Answer: C (メーッセージを残す**)**
Cisco FirepowerデバイスをVPNトラフィックのアクセス制御ポリシーをバイパスするように設定すると、デバイスはVPNトラフィックを検査しないため、リソースを無駄に消費しません。これは、VPNトラフィックがCisco Firepowerデバイスのリソースを無駄に消費しないようにするための最適なオプションです。
参照：
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-c

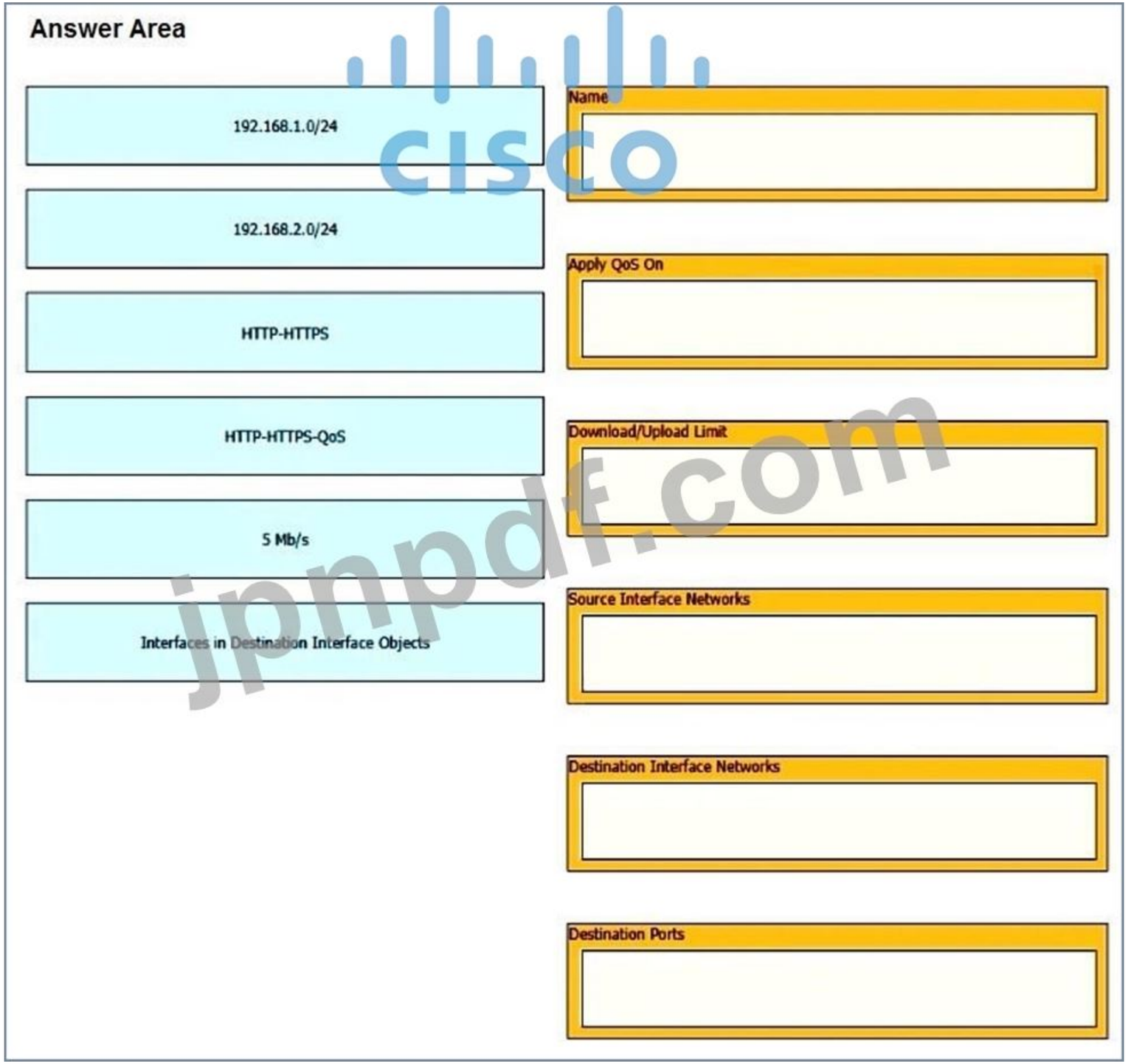
最新問題: **255**

ドラッグアンドドロップの質問

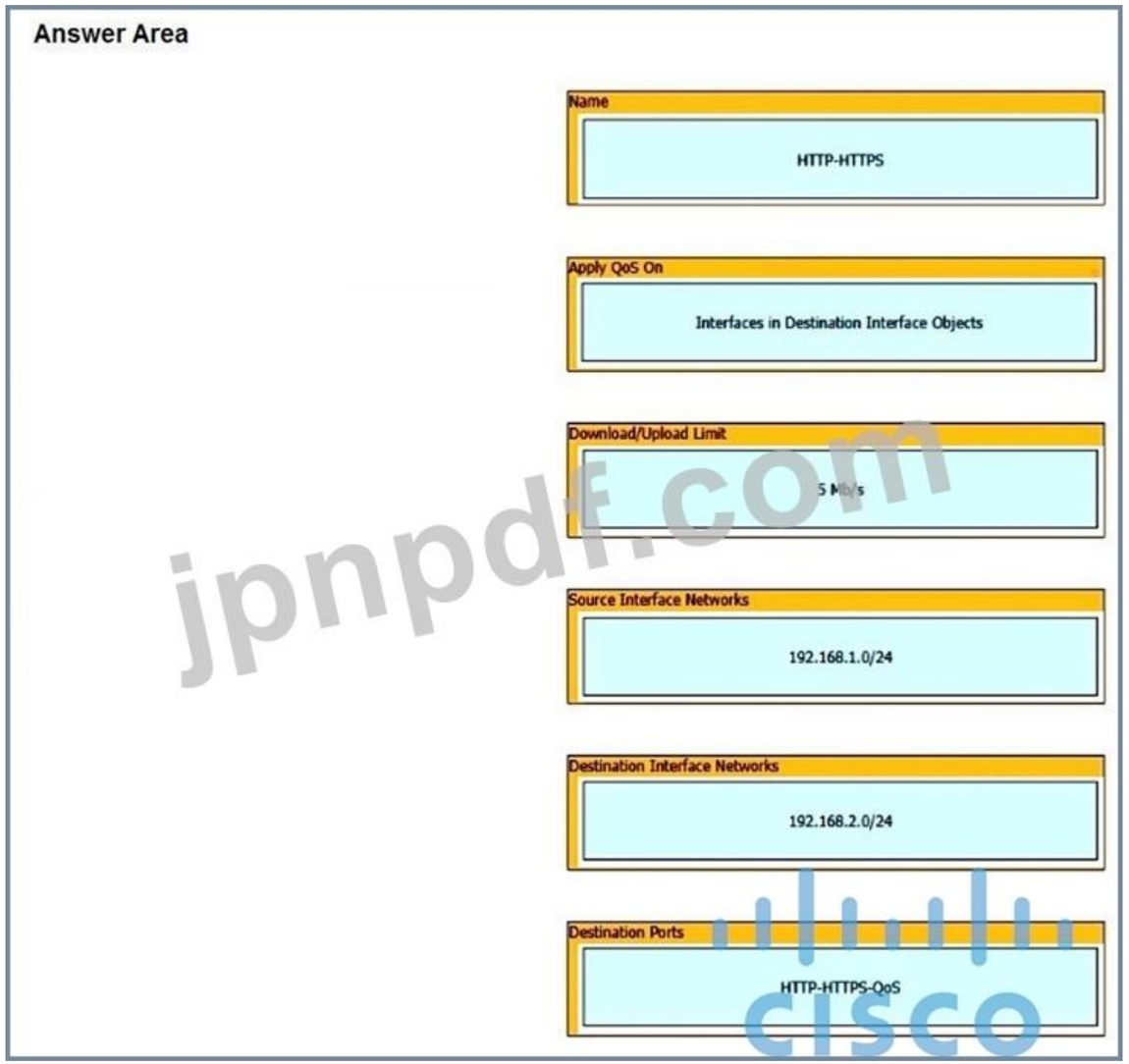
図を参照してください。エンジニアは、人事部門のユーザーからのHTTPおよびHTTPSトラフィックを制限するために、Cisco Firepower Management CenterでQoSポリシーを作成する必要があります。HTTPおよびHTTPSトラフィックのアップロードとダウンロードの制限は5Mbpsに設定する必要があります。左側の値を右側の対応する設定にドラッグ＆ドロップしてください。



Answer Area



Answer:



最新問題: **256**

ある企業は、Cisco FMCで管理されるCisco FTDによる侵入防御の導入を進めています。より少ないルールで重大な状況のみを検出し、誤検知を回避するには、どのアクションを選択する必要がありますか？

A. 最大検出

B. セキュリティよりも接続性を重視

C. バランスの取れたセキュリティと接続性

D. アクティブなルールはありません

Answer: B (メーッセージを残す**)**

最新問題**: 257**
Cisco FMC で設定され、Cisco FTD に伝播される 2 つの OSPF ルーティング機能はどれですか (2 つ選択してください)。
A. IPv6対応OSPFv2
B. OSPFパケットへのMD5認証
C. 仮想リンク
D. エリア境界ルータタイプ1 LSAフィルタリング
E. OSPFパケットへのSHA認証
Answer: B,C (メーッセージを残す**)**

最新問題**: 258**
アプリケーション層プリプロセッサにはどのようなものがありますか? (2 つ選択してください。)
A. DNP3
B. ICMP
C. CIFS
D. IMAP
E. SSL
Answer: (解答を表示する**)**

最新問題**: 259**
病院ネットワークでは、Cisco FMC管理対象デバイスのアップグレードと、災害復旧プロセスの確実な実施が求められています。ネットワークのダウンタイムを最小限に抑えるには、何をすべきでしょうか？
A. 冗長性を高めるためにISPへの2番目の回線を構成する
B. フェイルオーバー用にCisco FMCを構成する
C. Cisco FMC 管理対象デバイスをクラスタリング用に設定します。
D. バックアップとして使用するために現在の構成のコピーを保持します
Answer: D (メーッセージを残す**)**

最新問題**: 260**

The following applications have been identified as associated with attacks. You should identify applications in this lis
hat have low business relevance and evaluate whether it would be helpful to control them on your network.

Apps Associated with High Impact Events	Count
DNS	16
Internet Explorer	14
Web browser	8
FTP client	6
NetBIOS-ssn (SMB) client	6

Apps Associated with Low Impact Events	Count
Chrome	283
Internet Explorer	110
DCE/RPC client	74
Web browser Firefox	47
Firefox	36

TOP ATTACKERS AND TARGETS

The top attackers and target machines observed in the attack attempts on your network are listed below. For high
mpact attacks in particular, you should ensure that targets are well protected from potential attackers by patching
hese machines and blocking potentially malicious traffic.

High Impact Events

Attackers	Attacks
5.196.214.27	3
10.1.115.12	3
10.1.115.12	3
10.1.26.6	2
10.1.39.21	2

Targets	Attacks
31.31.196.236	6
185.118.166.155	6
37.48.82.212	4
185.86.77.12	4
192.161.54.60	4

図を参照してください。セキュリティエンジニアは組織のセキュリティを強化する必要があり、経営陣に承認を得るためにリスク軽減戦略を策定しています。この攻撃リスクレポートに基づいて、セキュリティエンジニアはどのようなアクションを取る必要がありますか？

A. NetBIOS をブロックします。

B. TCP ポート 80 のトラフィックを検査します。

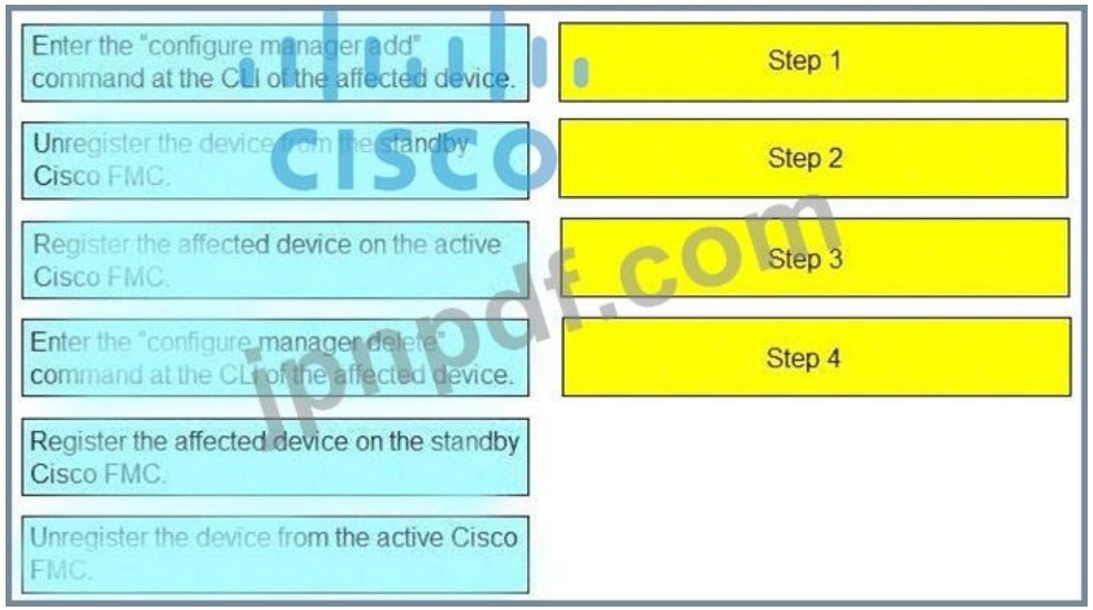
C. Internet Explorer をブロックします。

D. DNS トラフィックを検査します。

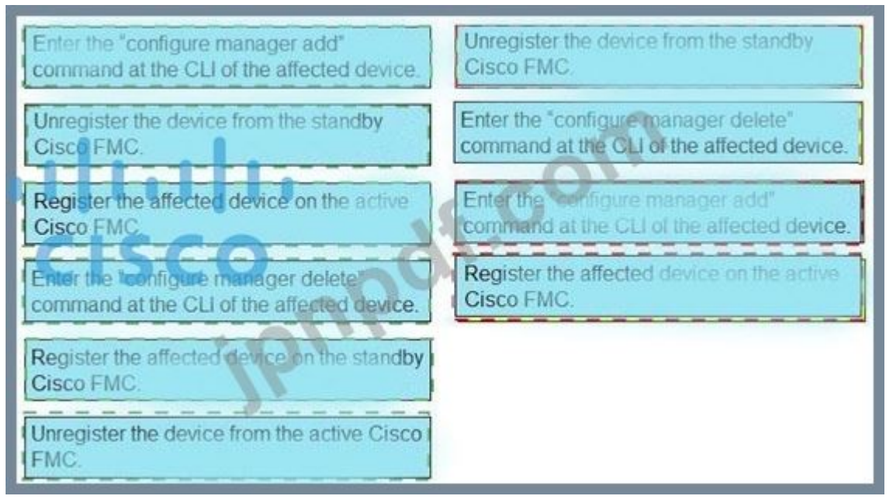
Answer: B (メーッセージを残す**)**

最新問題**: 261**

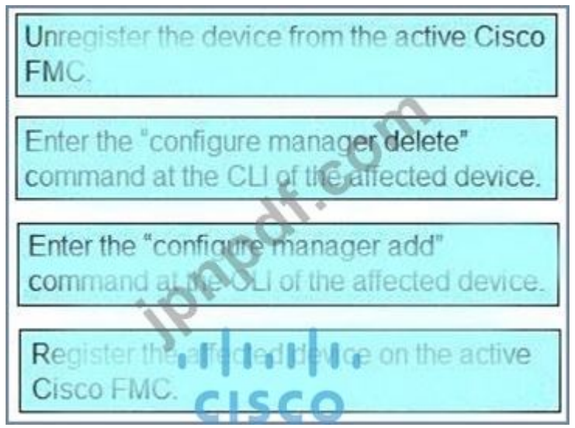
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。


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

Answer:


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

説明



説明
参考 :https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

最新問題: **262**
セキュリティエンジニアが従業員のメールアドレスから不審なファイルを発見し、分析のためにアップロードしようとしましたが、アップロードに失敗しています。最終登録ステータスは依然としてアクティブです。この問題の原因は何でしょうか？
A. Cisco AMP for Networks はオンプレミスの Cisco Threat Grid に接続できません。
B. Cisco AMP for Networks は Cisco Threat Grid Cloud に接続できません。
C. ホスト制限が設定されています。
D. ユーザーエージェントのステータスは監視に設定されています。
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config -76/network-malware- protection.html?bookSearch=true#:~:text=Threat%20Grid

最新問題: **263**
Cisco FTD のブリッジ グループ インターフェイスに関する次の 2 つの記述のうち正しいものはどれですか。(2 つ選択してください。)
A. ブリッジ グループは、透過型ファイアウォール モードとルーティング型ファイアウォール モードの両方でサポートされます。
B. ブリッジ グループ メンバーを使用する場合、双方向転送検出エコー パケットは FTD を介して許可されます。
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. 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。
E. 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存在する必要があります。
Answer: A,D (メーッセージを残す**)**

最新問題: **264**
FlexConfig を使用せずに Firepower Threat Defense でサポートされる 2 つの動的ルーティング プロトコルはどれですか。
（2つ選択してください。）
A. EIGRP
B. OSPF
C. 静的ルーティング

D. IS-IS
E. BGP
Answer: B,E (メーッセージを残す)
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660
/fptd- fdm-routing.html

最新問題: **265**
ネットワーク管理者は、Cisco FTDの背後にあるルータへのサイト間IPsec VPNを設定しています。管理者は、このデバイスへのUDPトラフィックを許可するアクセスポリシーを設定しています。
500、4500、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には、どのような操作が必要ですか？
A. 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。
B. アクセス ポリシーで IPsec 検査を有効にします。
C. 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。
D. アクセス ポリシーを変更して、すべてのポートを許可します。
Answer: C (メーッセージを残す)
1 台のルータが Cisco FTD (Firepower Threat Defense) ファイアウォールの背後にあるサイト間 IPsec VPN 構成では、適切な NAT トラバーサルが重要です。
アクセス ポリシーで UDP 500 (ISAKMP)、UDP 4500 (NAT-T)、および ESP (IP プロトコル 50) を許可している場合でも、適切に処理しないと NAT によって VPN が切断される可能性があります。

最新問題: **266**
クラスターユニット環境でサイト間 VPN を設定する場合の欠点は何ですか?
A. 障害が発生したマスター ユニットが回復した場合にのみ、VPN 接続を再確立できます。
B. すべてのクラスタ ユニット間で同時に VPN 接続を維持するには、スマート ライセンスが必要です。
C. 新しいマスター ユニットが選出された場合、VPN 接続を再確立する必要があります。
D. 新しいマスター ユニットが選出されると、確立された VPN 接続のみが維持されます。
Answer: (解答を表示する)
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster- solution.html#concept_g32_yml_y2b

最新問題: **267**
展示品を参照してください。


Cisco Secure Firewall Threat Defense（FTD）デバイスが、インラインセットを使用してインラインモードで導入されています。ネットワークエンジニアは、ルーティング先のルータR1とセキュアFTDデバイス間のケーブルが切断された場合、ルータR2のルーティングテーブルから直接接続されたルートM 68.1.0/24を削除するように指示しています。エンジニアはどのような対応を取る必要がありますか？
1
A. Secure FTDデバイスにリンクの古さを伝播するオプションを実装する
B. R1 と R2 の間にルーティング プロトコルを確立します。
C. Secure FTD デバイス上のハードウェア バイパスを無効にします。
D. R2のGi0/2インターフェースに自動ステート機能を実装する

Answer: (解答を表示する**)**
ルータR1とSecure FTDデバイス間のケーブルが切断された際に、ルータR2が192.168.1.0/24への直接接続ルートをルーティングテーブルから削除するようにするには、ネットワークエンジニアがSecure FTDデバイスに 『リンク状態を伝播』オプションを実装する必要があります。このオプションにより、FTDはリンク状態の変化を隣接デバイスに伝播し、切断が認識され、それに応じてルーティングテーブルが更新されます。
手順:
* FMC 経由で FTD デバイス構成にアクセスします。
* 関連するインターフェースのインターフェース設定に移動します。
* R1 および R2 に接続されているインターフェースに対して 『リンク状態の伝播』オプションを有効にします。
* 変更を FTD デバイスに展開します。
この設定により、リンク状態の変更がルータ R2 に伝達され、切断されたルートをルーティング テーブルから削除するように要求されます。
参考資料:Cisco Secure Firewall Threat Defense 構成ガイド、インターフェイス設定とリンク状態の伝播に関する章。

最新問題**: 268**
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. ファイアウォール モードを透過に変更します。
B. CDP トラフィックを許可するファイアウォール ルールを作成します。
C. ファイアウォール モードをルーティングに変更します。
D. 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。
Answer: (解答を表示する**)**

最新問題**: 269**
セキュリティエンジニアは、SHA-256ハッシュでゼロデイマルウェア攻撃を検出するためにCisco Secure Endpointを導入しています。
47ea931f3e9dc23ec0b0885a80663e30ea013d493f8e88224b570a0464084628。アプリケーションがこのハッシュに基づいてアクションを実行できるようにするには、Cisco Secure Endpoint で何を設定する必要がありますか？
A. 相関ポリシー
B. アクセス制御ルール
C. 変換セット
D. カスタム検出リスト
Answer: D (メーッセージを残す**)**

最新問題**: 270**
中規模企業では、最近の買収によりネットワーク帯域幅の利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の増加に伴い、1台のCisco FTDアプライアンスの導入環境を拡張し、より大容量のシステムを構築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採用すべきでしょうか？
A. パフォーマンスを向上させるには、複数の Cisco FTD アプライアンスをファイアウォール クラスタリング モードで展開します。
B. 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。
C. パフォーマンスを向上させるために複数のCisco FTD HAペアを導入する
D. パフォーマンスを向上させるために、クラスタリングモードで複数のCisco FTD HAペアを展開します。
Answer: A (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_C8502505F840451C9E600F1EED9BC18E

最新問題: **271**
ある組織がネットワークに新しいCisco FTDアプライアンスを導入しようとしています。エンジニアは、同一IPサブネット内の2つのネットワークセグメント間のアクセスを設定するという任務を負っています。このタスクを完了するには、どの手順が必要ですか？
A. ブリッジ仮想インターフェイスに IP アドレスを割り当てます。
B. ブリッジ グループの名前を指定します。
C. ループを防ぐために BPDU パケットを許可します。
D. セグメントごとに個別のブリッジ グループを追加します。
Answer: A (メーッセージを残す**)**

最新問題: **272**
セキュリティ エンジニアは、複数のブランチ ロケーションに対してアクセス制御ポリシーを構成しています。これらのロケーションは共通のルール セットを共有し、各ロケーションでローカルに重要な内部ネットワーク サブネットを含む INSIDE_NET と呼ばれるネットワーク オブジェクトを使用します。各ロケーションでポリシーの一貫性を維持しながら、適用可能なルール内でローカルに重要なネットワーク サブネットのみを許可するには、どのような手法が考えられますか。
A. デバイスごとに一意のACPを作成する
B. Cisco Talosから更新される動的ACPを利用する
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ACPを作成する
D. ポリシー継承を利用する
Answer: (解答を表示する**)**

最新問題: **273**
ネットワークエンジニアがFirepower Threat DefenseでURLフィルタリングを設定しています。クラウドサービスとの通信を可能にするために、Firepower Management Centerのどのポート要件を検証する必要がありますか？ 2つ選択してください。）
A. 受信ポート TCP/443
B. 受信ポート TCP/80
C. 送信ポート TCP/443
D. 送信ポート TCP/8080
E. 送信ポート TCP/80
Answer: C,E (メーッセージを残す**)**

最新問題: **274**
高可用性の実行を一時的に停止するには、プライマリ Cisco FTD ユニットの CLI でどのコマンドを入力しますか?
A. 高可用性を無効にする
B. 高可用性再開を構成する
C. システムサポートネットワークオプション

D. 高可用性サスペンドを構成する
Answer: A (メーッセージを残す**)**

最新問題**: 275**
Cisco Secure Firewall Threat Defense リモート アクセス VPN で使用できる 2 つの機能はどれですか。
（2つ選択してください。）
A. LDAPSを使用してDuoの2要素認証を有効にする
B. クラスタモードでのCisco Secure Firewall 4100シリーズのサポート
C. SSLリモートアクセスVPNは、SSLポート443を使用して他のCisco FTD機能とのポート共有をサポートします。
D. ゼロタッチネットワーク展開のためのライセンス利用
E. RADIUS動的認証を使用したRapid Threat Containmentのサポート
Answer: A,E (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense は、LDAP や RADIUS などの外部認証サーバとの統合をサポートしており、これを使用して Duo などの 2 要素認証ソリューションを有効にし、VPN ログイン時のセキュリティを強化できます。
FTD リモート アクセス VPN は、RADIUS 認証変更 (CoA) または動的認証を活用して、侵害された VPN クライアントを迅速に分離または修復することにより、迅速な脅威封じ込め機能をサポートします。
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/vpn-remote-access.html

最新問題**: 276**
ネットワークエンジニアがFirepower Threat DefenseでURLフィルタリングを設定しています。クラウドサービスとの通信を可能にするために、Firepower Management Centerのどのポート要件を検証する必要がありますか？ （2つ選択してください。）
A. 送信ポート TCP/443
B. 受信ポート TCP/80
C. 送信ポート TCP/8080
D. 受信ポート TCP/443
E. 送信ポート TCP/80
Answer: A,E (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/SecurityInternet_Accessand_Communication_Ports.html

最新問題**: 277**
しきい値設定はどの 2 つの場所で設定できますか? (2 つ選択してください。)
A. 各IPSルール
B. ネットワーク分析ポリシー内でグローバルに
C. 侵入ポリシーごとにグローバルに
D. 各アクセス制御ルール
E. プリプロセッサごとに、ネットワーク分析ポリシー内
Answer: (解答を表示する**)**
セクション: 構成
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.pdf

最新問題**: 278**

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ました。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、どのアクションを実行すればよいでしょうか？
A. キャプチャトラフィックコマンドの後に–Tオプションを使用してトレースを指定します。
B. Cisco FMC CLI ではなく Cisco FMC GUI 内でトレースを実行します。
C. キャプチャトラフィックコマンドの一部として詳細オプションを使用します。
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。
Answer: (解答を表示する**)**
この問題を解決するには、captureコマンドを使用し、traceオプションを指定します。capture-trafficコマンドはトラフィックをキャプチャし、パケットキャプチャファイルに表示するのみで、Snort検出アクションは表示しません。
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with- firepower-threat-defense-f.html#anc29

最新問題**: 279**
図を参照してください。ネットワークエンジニアは、Cisco Secure Firewall Management Center で生成された、ネットワークセキュリティと効率的な帯域幅利用に焦点を当てたネットワークリスクレポートを分析しています。どのアプリケーションを制限すべきでしょうか。

HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
BitTorrent	230,431	High	Low	141212.0074025
Ubuntu Update Manager	30,620	Medium	Low	9937.3018802...
Tivoli	3,872,608	Very Low	Very High	5972.237919
SIP	130,389	Low	Medium	4073.94787107
upLynk	11	Medium	Medium	84.0107183

ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
SSL	11,926,818	Medium	Medium	1449773.319273
Kerberos	6,694,337	Very Low	High	16476.005748
SSH	727,527	High	Medium	72265.972372
Microsoft Azure	467,381	Medium	Very Low	149794.0941926
SFTP	361,783	Medium	Medium	3858.8765371

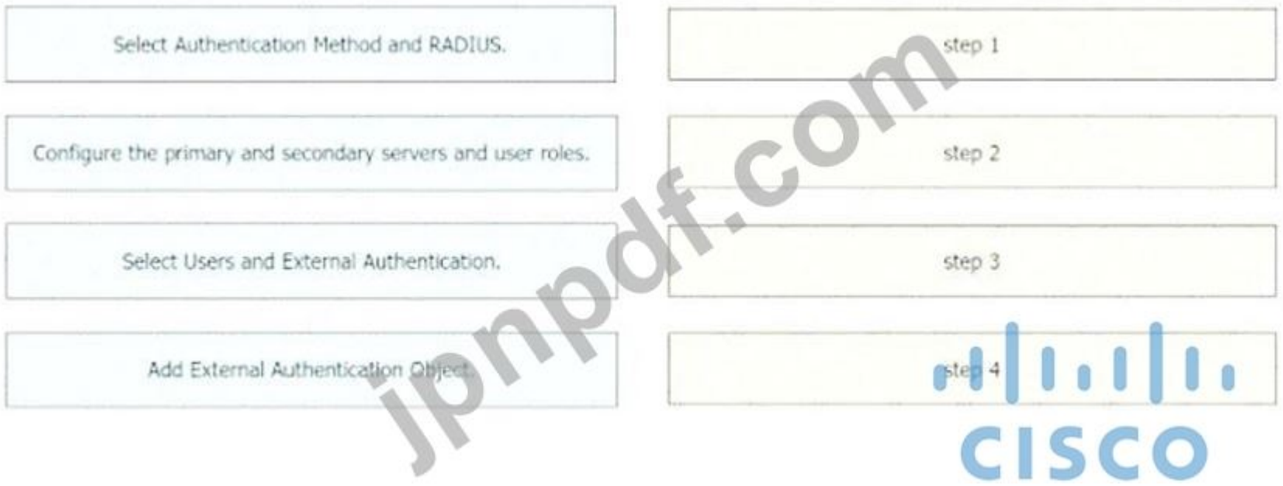
A. SFTP
B. ビットトレント
C. ティボリ
D. SSH
Answer: B (メーッセージを残す**)**

最新問題**: 280**
Cisco Firepower Management Center はいくつのレポート テンプレートをサポートしていますか?
A. 5
B. 無制限
C. 10
D. 20

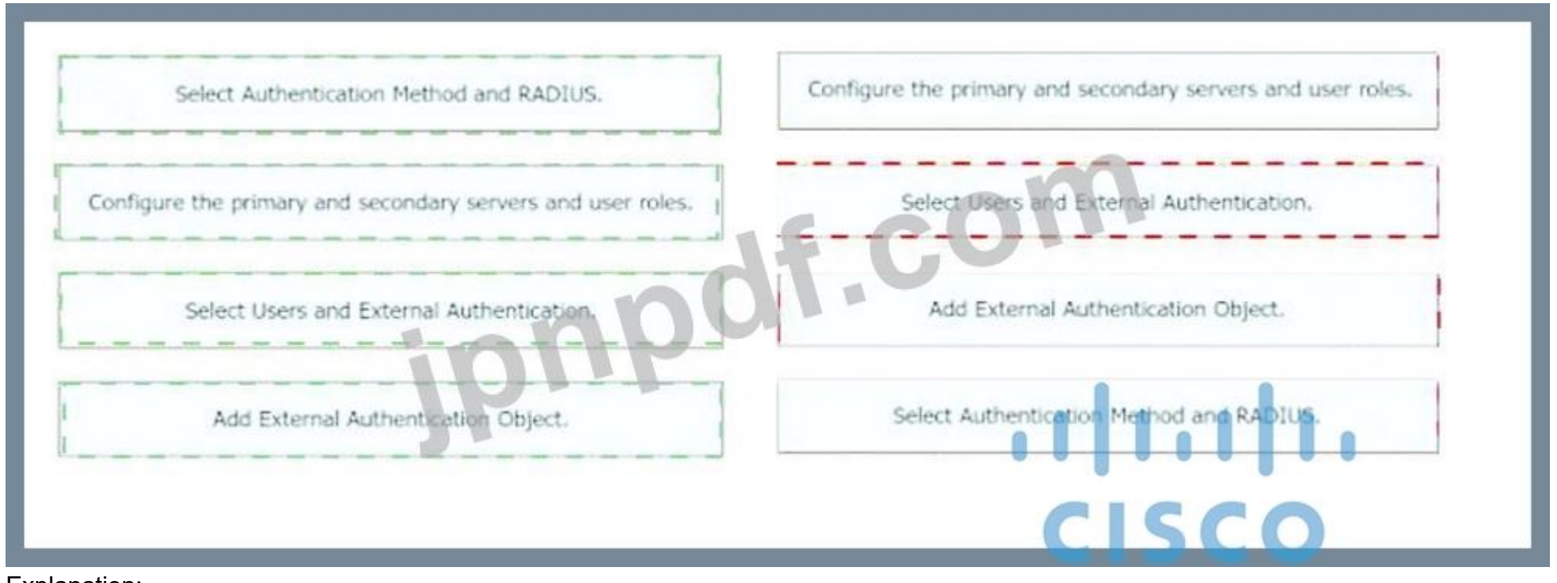
Answer: (解答を表示する)

最新問題: **281**
組織内のネットワークデバイスを管理 監視するためのネットワーク監視ツールを導入した後、Cisco FMCのMIBファイルを手動でアップロードする必要があることに気づきました。MIBファイルはどのフォルダにアップロードすればよいですか？
A. /etc/sf/DCMIB.ALERT
B. /sf/etc/DCEALERT.MIB
C. /etc/sf/DCEALERT.MIB
D. system/etc/DCEALERT.MIB
Answer: (解答を表示する)
セクション: 管理とトラブルシューティング
説明
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/Intrusion-External-Responses.pdf

最新問題: **282**
左側の設定手順を右側のシーケンスにドラッグ アンド ドロップして、Cisco FMC で RADIUS サーバーへの外部認証を有効にします。



Answer:



Explanation:
4、1、2、3

最新問題**: 283**
ネットワークエンジニアは、Cisco Secure Firewall Management Center と Cisco Secure Firewall Threat Defense 間の接続に問題があることを検出しました。初期トラブルシューティングの結果、ハートビートとイベントが受信されていないことが判明しました。エンジニアは両ピア間のセキュアチャネルを再確立しました。この問題を解決するために、エンジニアが実行する必要があるコマンドはどれですか？ 2つ選択してください。）
A. sudo stats_unified.pl
B. ディスクマネージャーを表示
C. 履歴を表示
D. manage_procs.pl
E. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
Answer: A,D (メーッセージを残す**)**

最新問題**: 284**
エンジニアは子ドメインでCisco FMCダッシュボードを設定する必要があります。ダッシュボードを親ドメインから表示するには、どのような操作を行う必要がありますか？
A. 別のタブを追加します。
B. ダッシュボードのコピーを作成します。
C. ポリシー継承設定を調整します。
D. 別のウィジェットを追加します。
Answer: B (メーッセージを残す**)**

最新問題**: 285**
管理者はCisco ASAからCisco FTDアプライアンスへの移行作業を進めており、トラフィックを中断することなく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ればよいでしょうか？

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
Answer: D (メーッセージを残す**)**
参照：
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

最新問題**: 286**
管理者はネットワークをより適切にセグメント化するためにインターフェースオブジェクトを作成しようとしていますが、オブジェクトにインターフェースを追加する際に問題が発生しています。この失敗の原因は何ですか？
A. インターフェースは複数のネットワークの NAT に使用されています。
B. 管理者は複数のタイプのインターフェースを追加しています。
C. 管理者は複数のゾーンにあるインターフェースを追加しています。
D. インターフェースは複数のインターフェース グループに属しています。
Answer: B (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4
インターフェース オブジェクト内のすべてのインターフェースは、すべて同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェース オブジェクトを作成した後は、含まれるインターフェースのタイプを変更することはできません。

最新問題**: 287**
パケット キャプチャによるトラブルシューティング中に、ファイル サイズ コマンド オプションが必要になるのはいつですか?
A. キャプチャパケットが32 MBを超える場合
B. キャプチャパケットが10 GBを超える場合
C. キャプチャパケットが二次メモリから制限されている場合
D. キャプチャパケットが16 MB未満の場合
Answer: A (メーッセージを残す**)**

最新問題**: 288**
展示品を参照してください。
エンジニアがアクセス制御ポリシーを変更して、ポリシーを通過するすべての DNS トラフィックを検査するルールを追加し、変更を加えてポリシーを展開したところ、DNS トラフィックが Snort エンジンによって検査されていないことがわかりました。
何ですか……
A. ルールのアクションは、許可ではなく信頼に設定されています。
B. ルールでは、トラフィックの発信元となるセキュリティ ゾーンを指定する必要があります。

C. ルールでは、検査の送信元ネットワークとポートを定義する必要があります。
D. ルールの送信元ポートの設定が間違っています。
Answer: A (メーッセージを残す**)**

最新問題**: 289**
エンジニアは、ネットワーク上の Cisco FTD デバイスによってブロックされているファイルのトラブルシューティングを行っています。
ユーザーは、ファイルは悪意のあるものではないと報告しています。
エンジニアは、ファイルを識別し、悪意のあるファイルかどうかを検証するためにどのようなアクションを実行しますか?
A. コンテキスト エクスプローラーを使用してファイルを検索し、調査のためにローカル マシンにダウンロードします。
B. 接続イベントを右クリックし、ファイルを AMP for Endpoints に送信して、ハッシュが悪意のあるものかどうかを確認します。
C. FMC ファイル分析を使用してファイルを検索し、[分析] を選択してその処置を決定します。
D. 侵入イベント内のファイルを識別し、分析のために Threat Grid に送信します。
Answer: D (メーッセージを残す**)**

最新問題**: 290**
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. FMC 内で設定する場合、両方のデバイスは同じドメイン内にある必要がある異なる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、異なるモデルである必要があります。
D. ユニットはファイアウォール ルーティング モードに対してのみ設定する必要があります。
E. ユニットは同じモデルである必要があります。
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

最新問題**: 291**
ネットワーク管理者は、Cisco Secure Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense インスタンスを、既知の暗号化ネットワークへのトラフィックをブロックするように設定したいと考えています。この要件を満たすには、管理者は Secure Firewall Management Center でどのシステム設定を行う必要がありますか？
A. アクセスポリシー。セキュリティインテリジェンス
B. マルウェア ポリシー。
C. ルール侵入ポリシー。セキュリティインテリジェンス
D. アクセスポリシー。ルール
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Management Center（FMC）が管理するCisco Secure Firewall Threat Defense（FTD）を使用して、既知の暗号通貨マイニングネットワークへのトラフィックをブロックするには、ネットワーク管理者がアクセス制御ポリシーでセキュリティ インテリジェンスを設定する必要があります。セキュリティ インテリジェンスにより、管理者は既知の悪意のあるIPアドレス、ドメイン、URLなどの脅威インテリジェンス フィードに基づいてトラフィックをブロックできます。
手順:
* FMC で [ポリシー] > [アクセス制御] > [アクセス制御ポリシー] に移動します。
* アクセス制御ポリシーを編集または作成します。
* セキュリティ インテリジェンス タブに移動します。

* 暗号通貨マイニング ネットワークを含む関連する脅威インテリジェンス フィードを有効にします。
* FTD デバイスにポリシーを適用します。
この構成により、既知の暗号通貨マイニング ネットワークへのトラフィックがブロックされ、暗号通貨マイニングの脅威に対するネットワークのセキュリティ体制が強化されます。
参考資料: Cisco Secure Firewall Management Center 構成ガイド、セキュリティ インテリジェンスの章。

最新問題: **292**
ファイアウォールが同じサブネットのレイヤー 2 とレイヤー 3 でトラフィックを転送できるようにするファイアウォール設計はどれですか。
A. Cisco Firepower Threat Defense モード
B. ルーティングモード
C. 統合ルーティングとブリッジング
D. 透過モード
Answer: (解答を表示する**)**

最新問題: **293**
Cisco FMC で再利用可能かつサポートされている 2 つのタイプのオブジェクトはどれですか (2 つ選択してください)。
A. HTTP および HTTPS GET 要求をレイヤー 7 アプリケーション プロトコルにリンクするのに役立つ動的キー 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 フィードとリスト、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、およびファイル リストを表すレピュテーションベースのオブジェクト
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、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/プロトコルペア、VXLANタグ、セキュリティゾーン、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カテゴリなどのレピュテーションベースのオブジェクト
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-00000414

最新問題: **294**
エンジニアはCisco FMCのリモートストレージを設定する必要があります。災害復旧のため、設定のバックアップはネットワーク上の安全な場所から利用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、エンジニアはどのような戦略を採用すべきでしょうか？
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。
Answer: C (メーッセージを残す**)**
説明
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/system
バックアップを 1 つのリモート システムに送信し、レポートを別のリモート システムに送信することはできませんが、どちらかをリモート システムに送信し、もう 1 つを Firepower Management Center に保存することはできます。

最新問題: **295**
ネットワーク管理者が月次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」と表示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のどこを確認すればよいでしょうか？

A. 分析 > ファイル > ネットワークファイル軌跡
B. 分析 > ホスト > ホスト属性
C. 分析 > ファイル > マルウェアイベント
D. 分析 > ホスト > 侵害の兆候
Answer: (解答を表示する**)**

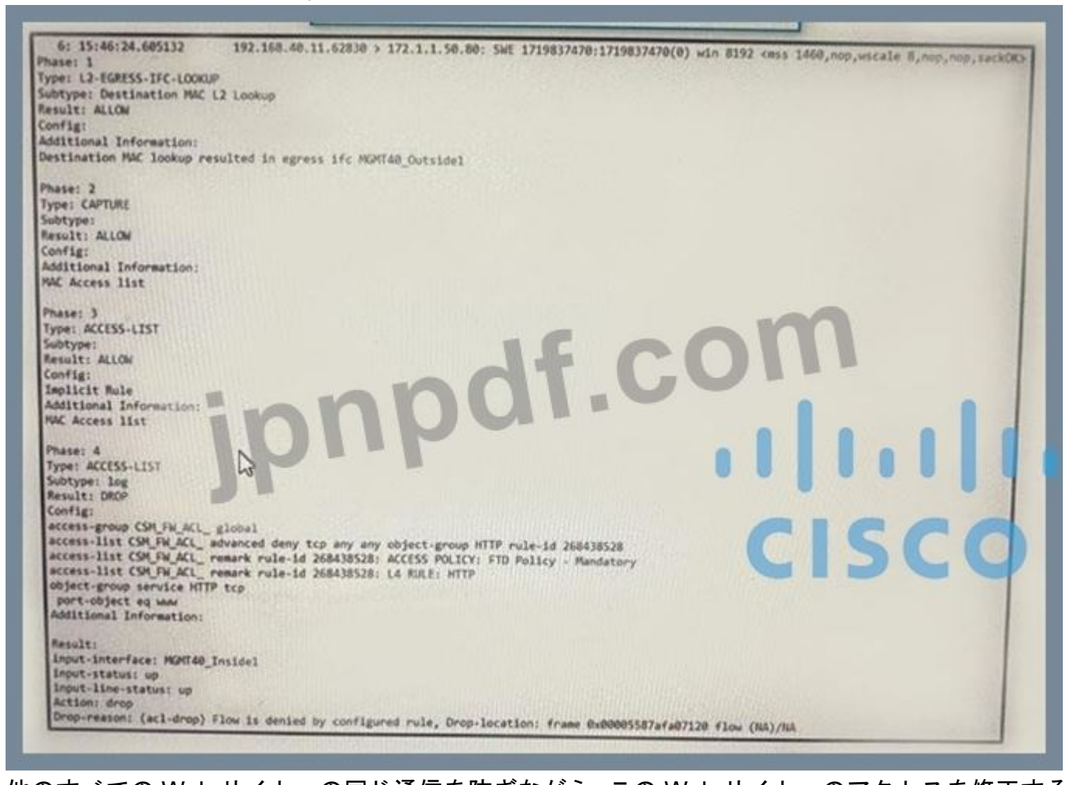
最新問題: **296**
エンジニアは、Cisco Secure Firewall Management Center を使用して Cisco セキュリティ デバイスを設定しています。
ローカル システム上の CA 証明書バンドルを Cisco サーバの最新の CA バンドルと比較するには、どの設定コマンドを実行する必要がありますか?
A. cert-update compare を設定する
B. 証明書更新テストを構成する
C. cert-update run-now を設定します
D. cert-update の自動更新を有効にする設定
Answer: (解答を表示する**)**

最新問題: **297**
IT管理者は、ネットワークエンジニアに対し、ネットワーク内のCisco FTDアプライアンスの高レベルな概要統計情報を提供するよう依頼しています。ビジネスはピークシーズンに近づいており、ビジネスの稼働時間を維持する必要性が高まっています。この情報を収集するには、どのレポートタイプを使用すればよいでしょうか？
A. マルウェアレポート
B. 標準レポート
C. SNMPレポート
D. リスクレポート
Answer: (解答を表示する**)**
このレポートはセキュリティ専門家以外の人向けであり、ピーク時の問題の解決に役立つ推奨事項が付属しています。
Firepower システムでは、次の 2 種類のレポートが提供されます。
リスク レポート - ネットワーク上で見つかったリスクの概要。
標準レポート - Firepower システムのあらゆる側面に関する詳細かつカスタマイズ可能なレポート。
リスクレポート
リスクレポートは、組織内で発見されたリスクを、持ち運びやすく、高レベルで分かりやすくまとめた要約です。これらのレポートを活用することで、システムへのアクセス権を持たない人や、ネットワークセキュリティの専門家ではない人にも、リスク領域に関する情報や、それらのリスクに対処するための推奨事項を共有できます。これらのレポートは、ネットワークセキュリティへの投資領域に関する議論を促進することを目的としています。

最新問題: **298**
Cisco ASA Firepowerモジュールを導入する際に、組織はネットワークに影響を与えることなくトラフィックの内容を評価したいと考えています。現在、物理アプライアンス上に同一デバイスのインスタンスを複数配置するように設定されています。組織のニーズを満たす導入モードはどれでしょうか？
A. インラインタップモニター専用モード
B. インラインモード
C. パッシブモニターのみモード
D. パッシブタップモニターのみのモード
Answer: (解答を表示する**)**

最新問題: **299**
ネットワーク管理者は、要求されたURL検索に基づいて悪意のあるサイトをブロックするデフォルトポリシーを設定したいと考えています。この要件を満たす機能はどれですか？
A. ファイルポリシー
B. マルウェアポリシー
C. DNSポリシー
D. URLフィルタリングポリシー
Answer: D (メーッセージを残す**)**
URL フィルタリングを使用すると、URL のカテゴリと評価に基づいて Web サイトへのアクセスを制御できます。これには、要求された URL を検査して悪意のあるサイトや危険なサイトをブロックすることも含まれます。
この機能は、カテゴリとレピュテーション ベースのフィルタリングを使用して、悪意のある URL または高リスクとして分類された URL を自動的にブロックし、デフォルトのブロック ポリシーの要件を満たすことができます。
URL フィルタリングは、HTTP/HTTPS トラフィックを検査し、URL を Cisco の URL データベースまたは手動で設定された URL リストと照合することによって機能します。
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/access-url-filtering.html

最新問題: **300**
展示品を参照してください。



他のすべての Web サイトへの同じ通信を防ぎながら、この Web サイトへのアクセスを修正するには、何をする必要がありますか?
A. Snort がポート 80 から 172.1.1 50 のみを許可するように侵入ポリシー ルールを作成します。
B. ポート443を172.1.1 50のみに許可するアクセス制御ポリシールールを作成します。
C. Snortがポート443を172.1.1.50のみに許可するように侵入ポリシールールを作成します。

D. ポート 80 を 172.1.1 50 のみに許可するアクセス制御ポリシー ルールを作成します。
Answer: D (メーッセージを残す**)**

最新問題**: 301**
病院ネットワークでは、Cisco FMC管理対象デバイスのアップグレードと、災害復旧プロセスの確実な実施が求められています。ネットワークのダウンタイムを最小限に抑えるには、何をすべきでしょうか？
A. Cisco FMC 管理対象デバイスをクラスタリング用に設定します。
B. フェイルオーバー用にCisco FMCを構成する
C. バックアップとして使用するために現在の構成のコピーを保持します
D. 冗長性を高めるためにISPへの2番目の回線を構成する
Answer: (解答を表示する**)**

最新問題**: 302**
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 IP アドレスに変換する NAT ポリシーを構成しました。
任意のソースがポート 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ました。
ウェブ サーバーは、ポート 80 でインターネットからまだアクセスできません。
どのような構成変更が必要ですか?
A. 送信元 IP アドレスと宛先 IP アドレスを変換するように NAT ポリシーを変更する必要があります。
B. 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。
C. ポート 80 の侵入ポリシーを無効にする必要があります。
D. アクション信頼に対してアクセス ポリシー ルールを構成する必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 303**
Cisco FTDには、BVIに割り当てられた2つの物理インターフェースがあります。各インターフェースは、同じスイッチ上の異なるVLANに接続されています。
Cisco FTD はどのファイアウォール モードをサポートするように設定されていますか?
A. 透明
B. アクティブ/アクティブフェイルオーバー
C. 高可用性クラスタリング
D. ルーティング
Answer: D (メーッセージを残す**)**
最新問題**: 304**
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ースにわたる最大 3 つの等コスト パスを持つ ECMP

C. 単一インターフェース上で最大3つの等コストパスを持つECMP
D. 透過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備えたBGPv4
Answer: (解答を表示する**)**
参照：
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

最新問題**: 305**
Cisco AMP for Endpoints では、どのオプションを選択すると、環境内で実行されたすべてのファイルのリストが表示されますか?
A. 脆弱なソフトウェア
B. ファイル分析
C. 検出
D. 有病率
E. 脅威の根本原因
Answer: (解答を表示する**)**

最新問題**: 306**

エンジニアは新しい Firepower の展開を設定しており、実装を開始するためにデフォルトの FMC ポリシーを確認しています。組織は、最初の試用フェーズで、ネットワーク トラフィックの大部分を通過させながら、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。どのデフォルト ポリシーを使用する必要がありますか。
A. 最大検出
B. セキュリティよりも接続性を重視
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html
C. バランスの取れたセキュリティと接続性
D. 接続性よりもセキュリティを重視
Answer: C (メーッセージを残す**)**

最新問題: **307**
エンドポイントで重大な脅威が検出されると、Cisco Identity Services Engine に感染したエンドポイントを手動または自動で封じ込めるように指示する 2 つのテクノロジーはどれですか (2 つ選択してください)。
A. シスコ ステルスウォッチ
B. シスコ FMC
C. シスコ AMP
D. Cisco ASA 5500 シリーズ
E. Cisco ASR 7200 シリーズ
Answer: (解答を表示する**)**

最新問題: **308**
ネットワーク管理者は、ルーテッドFTD上でBVIインターフェースを設定しようとしています。管理者は、ブリッジグループに接続されたインターフェース上のトラフィックを分離し、FTDがルーティングテーブルを使用してこのトラフィックをルーティングしないようにしたいと考えています。どのような設定が必要ですか？
A. BVIに接続された物理インターフェースからIPルーティングを削除する必要があります
B. BVIインターフェース用に新しいVRFを作成する必要があります
C. BVIにIPアドレスを設定する必要があります
D. BVIインターフェースは透過モードに設定する必要があります
Answer: D (メーッセージを残す**)**

最新問題: **309**
アクセス制御ポリシー内で使用されるオブジェクトを編集した後、どのような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. アクセス制御ポリシーの 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。
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

最新問題: **310**
アクセス制御ポリシー ルールで使用できる 2 つのアクションはどれですか (2 つ選択してください)。
A. すべてをブロック
B. 分析

C. モニター
D. 発見
E. リセット付きブロック
Answer: C,E (メーッセージを残す**)**

最新問題**: 311**
Cisco FMC で設定され、Cisco FTD に伝播される 2 つの OSPF ルーティング機能はどれですか。
（2つ選択してください。）
A. IPv6対応OSPFv2
B. 仮想リンク
C. OSPFパケットへのSHA認証
D. エリア境界ルータタイプ1 LSAフィルタリング
E. OSPFパケットへのMD5認証
Answer: B,E (メーッセージを残す**)**
Firepower Threat Defense デバイスは、次の OSPF 機能をサポートしています。
エリア内ルート、エリア間ルート、および外部 (タイプ I およびタイプ II) ルート。
仮想リンク。
LSA フラッディング。
OSPF パケットへの認証 (パスワードと MD5 認証の両方)。
Firepower Threat Defenseデバイスを指定ルータまたは指定バックアップルータとして設定します。Firepower Threat DefenseデバイスはABRとしても設定できます。
スタブ領域とそれほどスタブではない領域。
エリア境界ルータ タイプ 3 LSA フィルタリング。
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/ospf_for_firepower_threat_defense.html

最新問題**: 312**
ネットワークエンジニアは、トラフィックを検査しIDSとして機能するために、Secure Firewall Threat DefenseデバイスにIPSモードを設定する必要があります。エンジニアは既にSecure Firewall Threat Defenseデバイスのパッシブインターフェースとスイッチの SPANを設定しています。次にエンジニアは何を設定する必要がありますか？
A. セキュアファイアウォール脅威防御デバイスの侵入ポリシー
B. スイッチ上のアクティブなSPANポート
C. スイッチ上のDHCP
D. セキュアファイアウォール脅威防御デバイスのアクティブインターフェース
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスで IPS モードを設定してトラフィックを検査し、IDS として機能するには、ネットワーク エンジニアが FTD デバイスで侵入ポリシーを設定する必要があります。
スイッチのパッシブインターフェースとSPANはすでに設定済みで、トラフィックはFTDにミラーリングされています。次のステップは、悪意のあるトラフィックを検出して対応するためのルールとアクションを定義する侵入ポリシーを設定することです。
手順:
FMC で、[ポリシー] > [侵入] に移動します。
新しい侵入ポリシーを作成するか、既存の侵入ポリシーを編集します。
脅威を検出するためのルールとアクションを定義します。

侵入ポリシーを関連するインターフェースまたはアクセス制御ポリシーに適用します。この設定により、FTDはミラーリングされたトラフィックを検査し、定義された侵入ポリシーに基づいて適切なアクションを実行できるようになります。

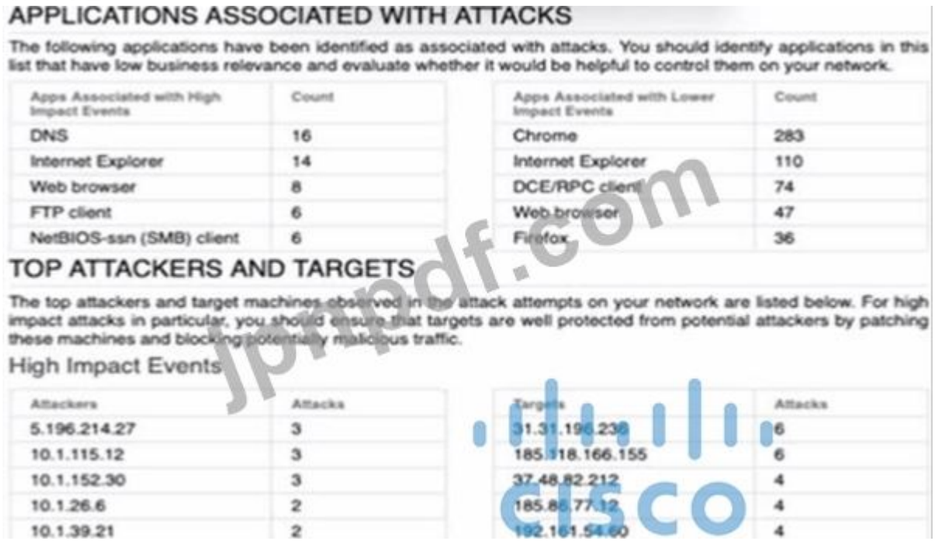
最新問題: **313**
エンジニアが接続問題のトラブルシューティングのためにCisco FTDでトラフィックをキャプチャすると、GUIツールで大量の出力データが表示されます。エンジニアは、この方法でキャプチャデータを表示するのは時間がかかり、分析やフィルタリングも難しいことに気づきました。この種の分析用に構築されたツールでデータを確認するには、どのファイル形式でデータをエクスポートする必要がありますか？
A. NetFlow v9
B. PCAP
C. NetFlow v5
D. IPFIX
Answer: (解答を表示する**)**
Cisco FTDデバイスでトラフィックをキャプチャして接続の問題をトラブルシューティングする場合、この種の分析用に構築されたツールを使用して確認するためにエクスポートできるファイル形式はPCAPです。PCAPはPacket Captureの略で、ネットワークインターフェースからキャプチャされたネットワークパケットデータを保存するために使用されるファイル形式です8。PCAPファイルには、各パケットのヘッダーとペイロードを含む、ネットワークパケットの生データが含まれています8。
PCAPファイルは、ネットワーク分析やトラブルシューティングのタスクで広く使用されています。ネットワーク管理者、アナリスト、研究者は、PCAPファイルを使用することで、ネットワークの問題の診断、悪意のあるアクティビティの検出、ネットワークパフォーマンスの測定、ネットワークプロトコルの理解など、様々な目的でネットワークトラフィックを検査 分析することができます8。PCAPファイルは、Wireshark、tcpdump、CA NetMaster、Microsoft Network Monitor8など、この形式に対応するアプリケーションで読み取ることができます8。
その他のオプションは、次の理由により正しくありません。
* NetFlow v9はファイル形式ではなく、ネットワークフローに関する情報を収集してエクスポートするためのプロトコルです。ネットワークフローとは、送信元および宛先IPアドレス、ポート、プロトコルなどの共通属性を持つパケットのシーケンスです9。NetFlow v9レコードには、開始時刻と終了時刻、バイト数、パケット数など、ネットワークフローに関する概要情報が含まれています9。NetFlow v9レコードには、ネットワークパケットの生データは含まれていません。
* NetFlow v5はファイルタイプではなく、ネットワークフローに関する情報を収集およびエクスポートするためのNetFlowプロトコルの以前のバージョンです。NetFlow v5レコードにはNetFlow v9レコードと同様の情報が含まれますが、フィールド数が少なく、柔軟性が低くなっています10。NetFlow v5レコードには、ネットワークパケットの生データは含まれません。
* IPFIX はファイル形式ではなく、ネットワークフローに関する情報を収集してエクスポートするためのプロトコルです。IPFIX は IP Flow Information Export の略で、NetFlow v9 をベースにいくつかの拡張と改良が加えられています11。IPFIX レコードには NetFlow v9 レコードと同様の情報が含まれていますが、フィールド数が多く、柔軟性も高くなっています11。IPFIX レコードには、ネットワークパケットの生データは含まれません。

最新問題: **314**
Cisco AMP for Networks の展開において、クラウドに到達できない場合、どのような処理が返されますか?
A. 利用できません
B. クリーン
C. 切断されました
D. 不明
Answer: D (メーッセージを残す**)**

最新問題: **315**
エンジニアがCisco FMC上でネットワーク検出ポリシーを設定しました。設定時に、データベースに過剰なイベントが記録され、Cisco FMCに過負荷がかかっていることがわかりました。監視対象のNATデバイスが、短期間のうちにオペレーティングシステムのアップデートを複数回実行しています。この問題を軽減するには、どのような設定変更が必要ですか？
A. ロードバランサーと NAT デバイスを除外します。
B. 方式を TCP/SYN に変更します。

C. NAT デバイス上のエントリ数を増やします。
D. デフォルトのネットワークのままにします。
Answer: A (メーッセージを残す**)**

最新問題**: 316**
Cisco Secure Client 経由で Cisco Secure Firewall Threat Defense デバイスの背後にある企業ネットワークに接続しているリモートユーザーから、ソフトフォンを使用してリモートユーザー間で通話する際に音声が聞こえないという報告があります。同じユーザーが企業ネットワーク内の社内ユーザーには問題なく通話できます。この問題の原因は何ですか？
A. Cisco Secure Firewall Threat Defenseでハブ経由のスポーク間接続を有効にするオプションが選択されていません
B. Cisco Secure Firewall Threat Defenseには、外部から外部への通信を許可するNATポリシーが必要です。
C. ヘアピニング機能はCisco Secure Firewall Threat Defenseでは利用できません
D. Cisco Secure Firewall Threat DefenseのリモートアクセスVPNでスプリットトンネリングが有効になっています
Answer: C (メーッセージを残す**)**

最新問題**: 317**

APPLICATIONS ASSOCIATED WITH ATTACKS
The following applications have been identified as associated with attacks. You should identify applications in this list that have low business relevance and evaluate whether it would be helpful to control them on your network.

Apps Associated with High Impact Events	Count
DNS	16
Internet Explorer	14
Web browser	8
FTP client	6
NetBIOS-ssn (SMB) client	6

Apps Associated with Lower Impact Events	Count
Chrome	283
Internet Explorer	110
DCE/RPC client	74
Web browser	47
Firefox	36

TOP ATTACKERS AND TARGETS
The top attackers and target machines observed in the attack attempts on your network are listed below. For high impact attacks in particular, you should ensure that targets are well protected from potential attackers by patching these machines and blocking potentially malicious traffic.
High Impact Events

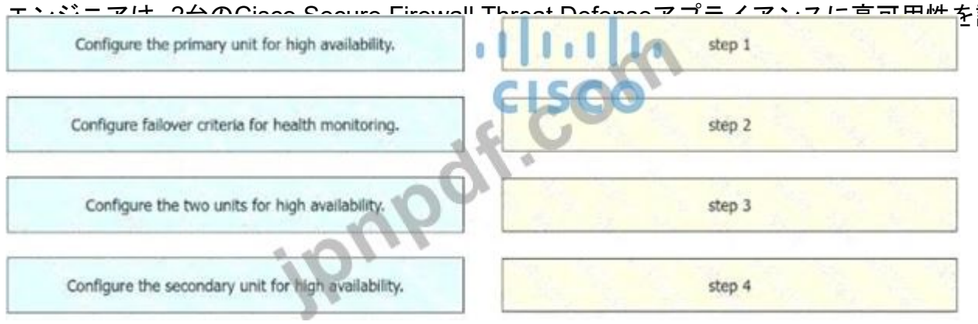
Attackers	Attacks
5.196.214.27	3
10.1.115.12	3
10.1.152.30	3
10.1.26.6	2
10.1.39.21	2

Targets	Attacks
31.31.196.236	6
185.118.166.155	6
37.48.82.212	4
185.86.77.12	4
192.161.54.60	4

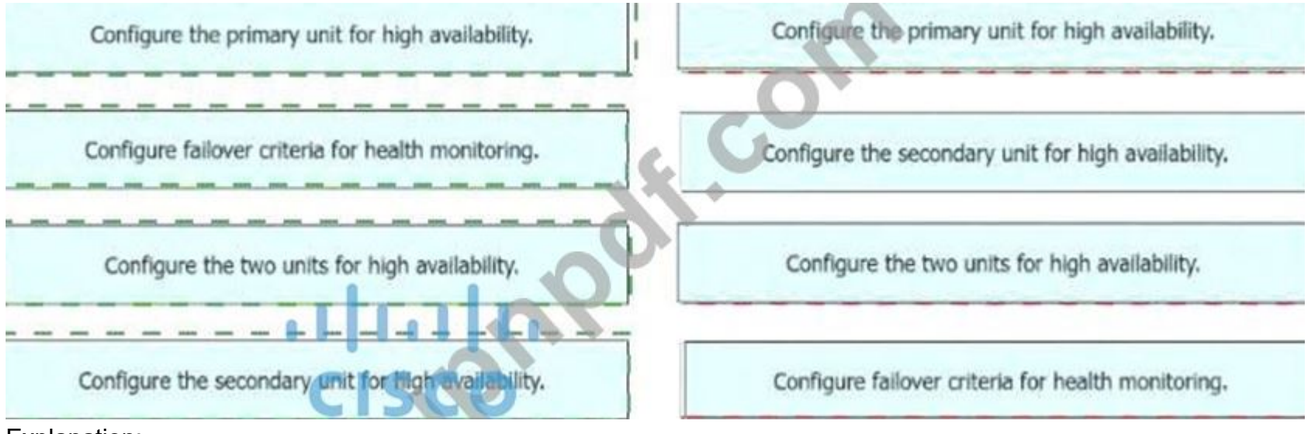
セキュリティエンジニアは組織のセキュリティを強化する必要があり、経営陣に承認を得るためにリスク軽減戦略を策定しています。この攻撃リスクレポートに基づいて、セキュリティエンジニアはどのようなアクションを取る必要がありますか？
A. DNSトラフィックを検査する
B. NetBIOS をブロックします。
C. 内部エクスプローラーをブロックする
D. TCPポート80のトラフィックを検査する
Answer: A (メーッセージを残す**)**
攻撃リスクレポートによると、DNSは多数の影響イベント（16件）と関連付けられています。DNSトラフィックはネットワーク運用に不可欠ですが、DNSトンネリング、DDoS攻撃、データ窃盗などの悪意のある活動

に悪用される可能性もあります。セキュリティを強化するために、セキュリティエンジニアはDNSトラフィックの検査に重点を置く必要があります。これには、DNSセキュリティソリューションの導入とDNSトラフィックの異常監視が含まれ、潜在的な脅威を検出 軽減します。
手順:
* DNS フィルタリング、DNSSEC、DNS 異常検出などの DNS セキュリティ ツールを実装します。
* DNS トラフィックに悪意のあるアクティビティがないか検査するようにファイアウォールを構成します。
* 脅威を特定して対応するために、DNS ログを定期的に分析します。
このアクションは、レポートで特定された重大なリスクに対処し、DNS を悪用した潜在的な攻撃を軽減するのに役立ちます。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、DNS セキュリティとトラフィック検査の章。

最新問題: **318**
エンジニアは、2台のCisco Secure Firewall Threat Defenseアプライアンスに高可用性を設定する必要があります。設定手順を左側から右側のシーケンスにドラッグ＆ドロップしてください。



Answer:



Explanation:
ステップ1 プライマリユニットを高可用性用に構成する）、
ステップ2 セカンダリユニットを高可用性用に構成する）
ステップ3 2つのユニットを高可用性用に構成する）、
ステップ4 ヘルスモニタリングのフェイルオーバー基準を構成する）

最新問題: **319**
Cisco Threat Response におけるケースブック機能の役割は何ですか?
A. アラート機能付きトリアージオートマトン

B. アラートの優先順位付け
C. ブラウザ拡張機能経由でデータを取得する
D. 脅威アナリストの共有
Answer: D (メーッセージを残す**)**

最新問題**: 320**
展示品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ましたが、サーバーからの応答がありません。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保証するには、どのアクションを実行すればよいですか？
A. 検査後に ICMP トラフィックを許可するようにカスタム Snort 署名を設定します。
B. ICMP トラフィックを許可するように Snort ルールを変更します。
C. 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。
D. ICMP 許可リストを作成し、ICMP 宛先を追加して暗黙的な拒否リストから削除します。
Answer: C (メーッセージを残す**)**

最新問題**: 321**
Cisco AnyConnect 経由で Cisco FTD デバイスの背後にある企業ネットワークに接続するリモート ユーザーは、ソフトフォンを使用してリモート ユーザー間で通話するときに音声が聞こえないと報告しています。
同じユーザーは、企業ネットワーク上の社内ユーザーには問題なく電話をかけることができます。この問題の原因は何でしょうか？
A. ヘアピン機能は FTD では使用できません。
B. FTDのリモートアクセスVPNでスプリットトンネリングが有効になっています
C. FTDには外部から外部への通信を許可するNATポリシーがありません
D. FTD でハブを介したスポーク間接続を有効にするオプションが選択されていません。
Answer: C (メーッセージを残す**)**
Cisco FTD デバイスの背後で AnyConnect VPN 経由で接続されたリモート ユーザーの場合、リモート ユーザー間の通話には、VPN クライアントが論理的に外部インターフェイス上にあるため 「外部から外部」へのトラフィックと見なされる VPN クライアント間のトラフィックを FTD が許可する必要があります。
この外部から外部への通信を許可する適切な NAT 免除または NAT ポリシーがないと、リモート ユーザー間のトラフィックがブロックまたはドロップされ、通話中に音声が聞こえないなどの問題が発生します。
Cisco FTD では、このような通信を許可するために明示的な NAT ルールが必要です。そうでない場合、デフォルトの動作によってこのトラフィックがブロックされます。
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/216180- トラブルシューティング-common-anyconnect-communication.pdf

最新問題**: 322**
FTD ユニットを IP アドレス 10.0.0.10 にあり、登録キー Cisco123 を持つ FMC マネージャに関連付けるには、FTD ユニットでどのコマンドを実行しますか?
A. マネージャのローカル 10.0.0.10 Cisco123 を設定します
B. マネージャの設定にCisco123 10.0.0.10を追加します
C. マネージャのローカル Cisco123 10.0.0.10 を設定します。
D. マネージャの設定に 10.0.0.10 Cisco123 を追加します
Answer: D (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

最新問題: **323**
ネットワークエンジニアがFirepower Threat DefenseでURLフィルタリングを設定しています。クラウドサービスとの通信を可能にするために、Firepower Management Centerのどの2つのポート要件を検証する必要がありますか？
（2つ選択してください。）
A. 送信ポート TCP/443
B. 受信ポート TCP/80
C. 送信ポート TCP/8080
D. 受信ポート TCP/443
E. 送信ポート TCP/80
Answer: A,E (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/セキュリティ

最新問題: **324**
ネットワーク管理者は先月のファイル レポートを確認し、exe を除くすべてのファイル タイプが削除されたことに気付きました。
不明な処理が表示されます。この問題の原因は何ですか？
A. マルウェア ライセンスが Cisco FTD に適用されていません。
B. Cisco FMC はインターネットに接続できず、ファイルを分析できません。
C. アクセス ポリシーにファイル ポリシーが適用されていません。
D. Spero ファイル分析のみが有効になります。
Answer: C (メーッセージを残す**)**
説明
ファイルポリシーは、Cisco Firepower Threat Defense（FTD）デバイスが様々なタイプのファイルに遭遇した際に実行するアクションを定義します。ファイルポリシーは、アクセス制御ポリシーの一部として適用されます。アクセス制御ポリシーにファイルポリシーが含まれていない場合、FTDデバイスは遭遇したファイルに対して何のアクションも実行せず、exeファイルを除くすべてのファイルタイプに対して「不明」という処理結果を返します。
参照：
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-c

最新問題: **325**
Cisco Firepower システムでは、アクセス制御ポリシーはどのような 2 つの方法で動作しますか? (2 つ選択してください。)
A. 構成の変更が展開されると、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、その後に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、関連付けられた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に対して予備検査を実行し、信頼できるパラメータと一致するかどうかを検証します。
Answer: A,C (メーッセージを残す**)**
セクション: 構成
説明/参照: 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

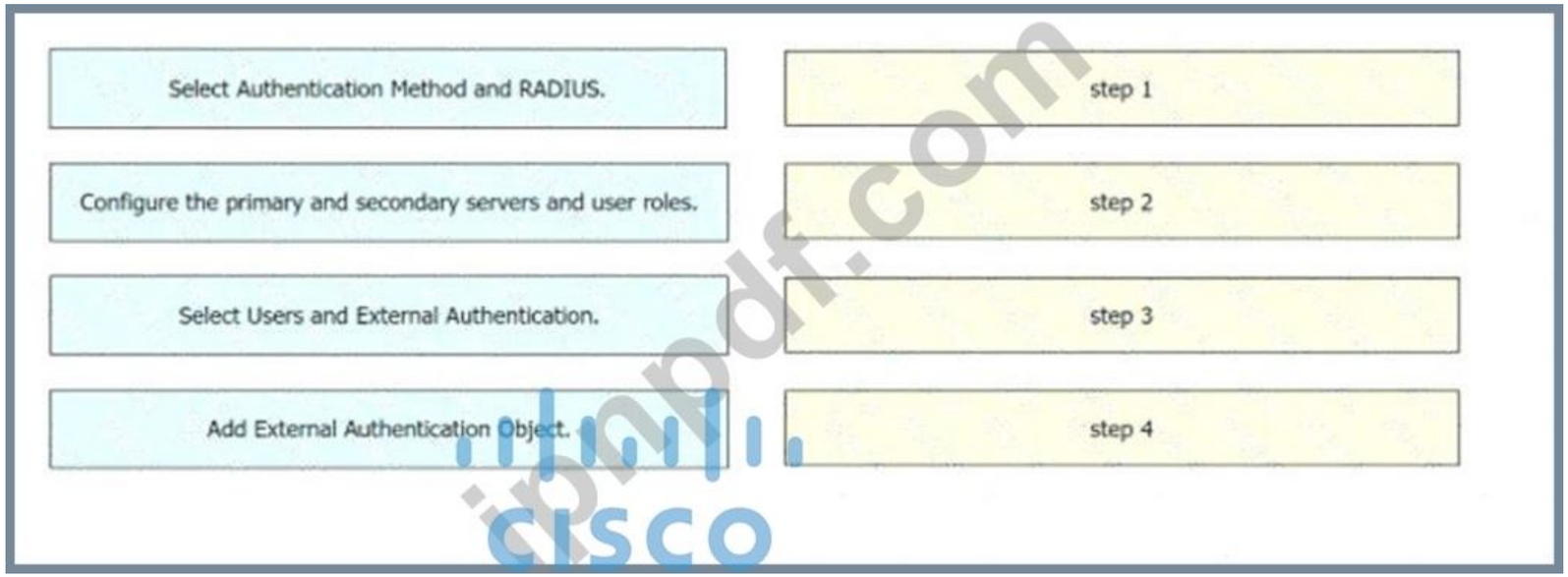
最新問題: **326**

ネットワーク エンジニアは、別の IP サブネットを作成せずにトラフィック検査のために FTD デバイスを介してユーザー セグメントを拡張しています。これは、ルーティング モードの FTD デバイスでどのように実現されるのでしょうか。
A. ARPを利用してトラフィックをファイアウォールに誘導する
B. インラインセットインターフェースを割り当てることによって
C. BVIを使用して、ユーザーセグメントと同じサブネットにBVI IPアドレスを作成します。
D. 事前フィルタルールを活用してプロトコル検査をバイパスする
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

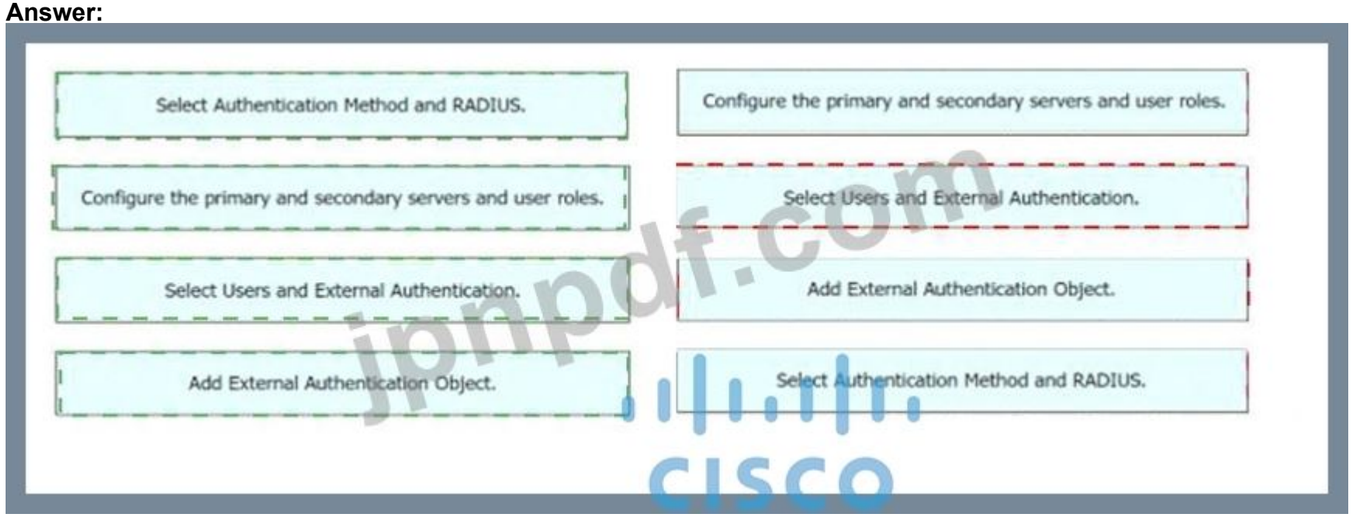
最新問題**: 327**
ネットワークセキュリティエンジニアは、問題のトラブルシューティングを行う際に、Cisco FMC Webブラウザからパケットキャプチャをエクスポートする必要があります。アドレス https://<FMC IP>/capture/CAPI/pcap/test.pcap にアクセスすると、PCAPファイルではなくエラー 「403: Forbidden」が表示されます。この問題を解決するには、エンジニアはどのような対応を取る必要がありますか？
A. ブラウザのプロキシ サーバ設定として Cisco FTD IP アドレスを使用します。
B. ブラウザのプロキシ設定を無効にします。
C. HTTPS サーバーを無効にして、代わりに HTTP を使用します。
D. デバイス プラットフォーム ポリシーに対して HTTPS サーバーを有効にします。
Answer: D (メーッセージを残す**)**

最新問題**: 328**
図を参照してください。エンジニアがCisco FMCのネットワークリスクレポートを分析しています。ネットワークの不正使用を防ぐために、エンジニアはどのアプリケーションに対して直ちに対策を講じる必要がありますか？
A. ケルベロス
B. クローム
C. TOR
D. YouTube
Answer: C (メーッセージを残す**)**

最新問題**: 329**
左側の設定手順を右側のシーケンスにドラッグ アンド ドロップして、Cisco FMC で RADIUS サーバーへの外部認証を有効にします。



Answer:



Explanation:

4、1、2、3

最新問題**: 330**

FTD を構成する際に、ネットワーク エンジニアは、アプライアンスを通過するトラフィックにルーティングや VLAN 書き換えが必要ないことを確認したいと考えています。

このタスクを実行するためにエンジニアはどのインターフェース モードを実装する必要がありますか?

A. 受動態

B. 透明

C. インラインタップ

D. インラインセット

Answer: (解答を表示する**)**

パッシブ: トラフィックは IPS を通過しません。
インライン タップ: パケットのコピーを取得しますが、トラフィックは IPS を通過しません。
透明: 透明なインライン モードなので、これも答えになります。
インラインセット :バンプオンワイヤモードと呼ばれます。トラフィックはアプライアンスを通過しますが、ルーティングやVLAN書き換えは必要ありません。
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

最新問題**: 331**
管理者はネットワークをより適切にセグメント化するためにインターフェースオブジェクトを作成しようとしていますが、オブジェクトにインターフェースを追加する際に問題が発生しています。この失敗の原因は何ですか？
A. インターフェースは複数のネットワークの NAT に使用されています。
B. 管理者は複数のタイプのインターフェースを追加しています。
C. 管理者は複数のゾーンにあるインターフェースを追加しています。
D. インターフェースは複数のインターフェース グループに属しています。
Answer: D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62
/再利用可能なオブジェクト.html#ID-2243-000009b4
インターフェース オブジェクト内のすべてのインターフェースは、すべて同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェース オブジェクトを作成した後は、含まれるインターフェースのタイプを変更することはできません。

最新問題**: 332**
Cisco FMC で再利用可能かつサポートされている 2 つのタイプのオブジェクトはどれですか (2 つ選択してください)。
A. FQDNマッピングとネットワーク、ポート/プロトコルペア、VXLANタグ、セキュリティゾーン、送信元/送信先の国を表すネットワークベースのオブジェクト
B. セキュリティ インテリジェンス フィードとリスト、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 リストを表すレピュテーションベースのオブジェクト
C. URLカテゴリなどのレピュテーションベースのオブジェクト
D. HTTP および HTTPS GET 要求をレイヤー 7 アプリケーション プロトコルにリンクするのに役立つ動的キー マッピング オブジェクト。
E. 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、発信国/宛先国を表すネットワークベースのオブジェクト
Answer: B,E (メーッセージを残す**)**

最新問題**: 333**
Cisco Firepower でファイアウォール デバッグ メッセージを生成するために使用される CLI コマンドはどれですか?
A. システムサポート ファイアウォールエンジン デバッグ
B. システムサポート ssl-debug
C. システムサポートプラットフォーム
D. システムサポートダンプテーブル

Answer: (解答を表示する**)**
セクション: 管理とトラブルシューティング
説明/参考資料: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower- management-center-display-acc.html

最新問題**: 334**
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
Answer: A (メーッセージを残す**)**
セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/firepower_command_line_reference.html

最新問題**: 335**
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
C. トリアージ
D. 保護
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html

最新問題**: 336**
展示をご覧ください。エンジニアがCisco Firepower Management Centerのダッシュボードを分析しています。
データ損失のリスクを減らすために、ユーザーはどのようなアクションを実行する必要がありますか?

Top Web Applications Seen

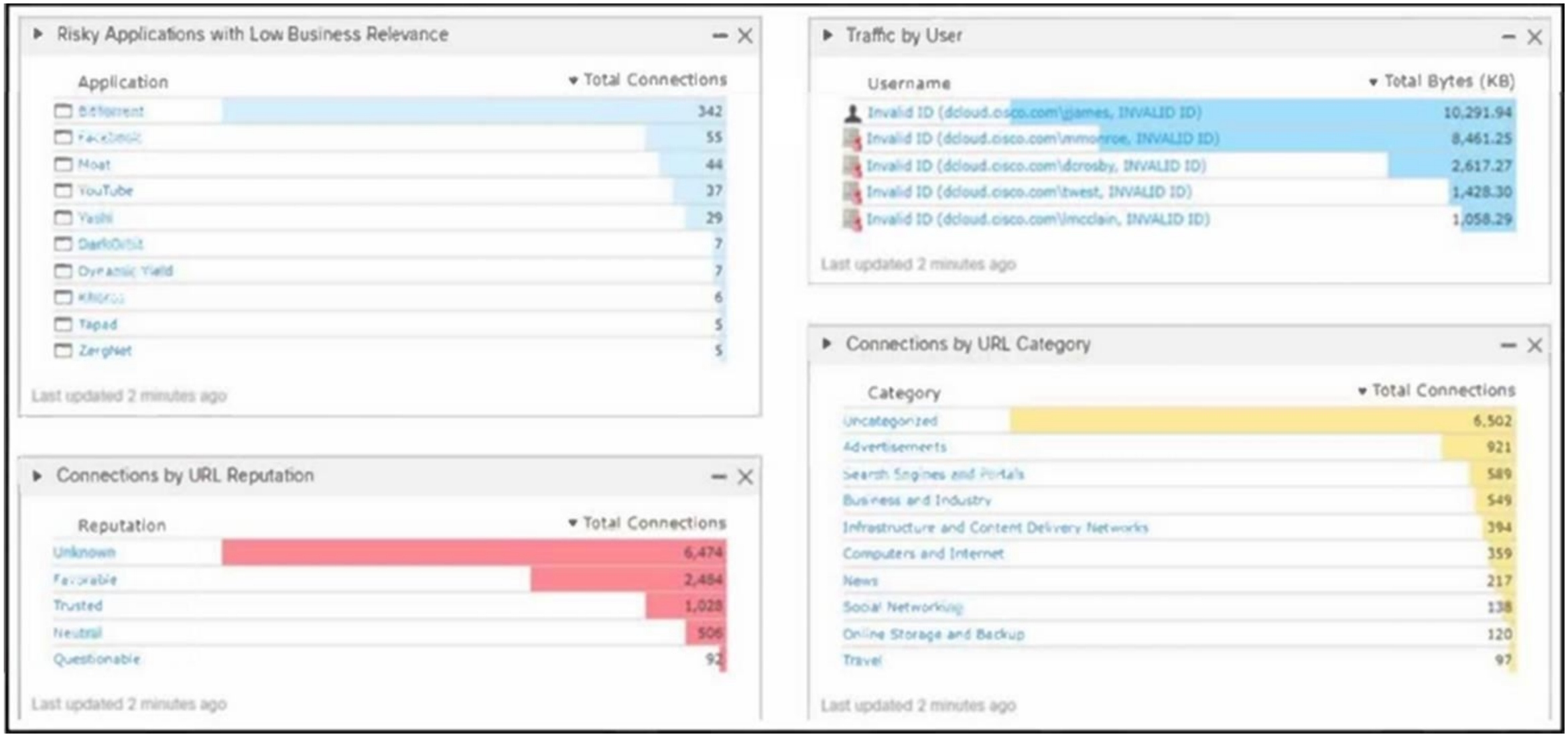
Application	Total Bytes (KB)
Google Play	12,249.52
Dropbox	10,778.64
The Huffington Post	10,145.08
JetBrains	6,754.41
Yahoo!	4,105.83
Amazon	3,750.49
YouTube	3,003.71
The New York Times	2,078.34
RealNetworks	2,009.26
Google	1,689.01
TripAdvisor	1,601.36
BBC	1,427.14
eBay	917.75
The Telegraph	854.16
Gmail	553.91

Last updated 5 minutes ago

Top Client Applications Seen

Application	Total Bytes (KB)
Chrome	53,275.58
Internet Explorer	26,121.09
SSL client	14,728.03
Google Update	12,222.16
Dropbox	10,778.64
JetBrains	6,754.41
Yahoo!	4,105.83
YouTube	3,003.71
Firefox	1,929.02
Pinterest	499.01
QUIC	286.83
Google Analytics	273.24
Twitter	203.93
Amazon Web Services	161.51
Safari	148.23

Last updated 5 minutes ago



A. 評判が不明な URL をすべて停止します。
B. Dropbox の使用をブロックします。
C. 分類されていないすべての URL を停止します。
D. すべての BitTorrent アプリケーションをブロックします。
Answer: D (メーッセージを残す**)**
BitTorrent トラフィックは、表示されているビジネス関連性の低いピアツーピア プロトコルの中で最もアクティブです。
BitTorrent をブロックすると、大量の管理されていないファイル転送が防止され、機密データの流出のリスクが大幅に軽減されます。

最新問題: **337**
エンジニアは、Cisco FTD ファイアウォールを介して単一の IP サブネットを接続し、ポリシーを適用したいと考えています。
内部 IP サブネットを外部に対して別の IP アドレスとして提示する必要があります。

これらの要件を満たすには何を構成する必要がありますか?
A. NAT を有効にして、Cisco FTD ファイアウォールをルーテッド モードで設定します。
B. ダウンストリーム ルーターを NAT を実行するように設定します。
C. NAT を有効にして、Cisco FTD ファイアウォールを透過モードで設定します。
D. 上流ルーターを NAT を実行するように設定します。
Answer: A (メーッセージを残す**)**

最新問題**: 338**
ネットワークエンジニアは、Cisco Secure Firewall Threat DefenseデバイスにIPSモードを設定してトラフィックを検査し、IDSとして機能するようにする必要があります。エンジニアは既に、セキュアファイアウォール Threat Defenseデバイスのパッシブインターフェースとスイッチのスパンを設定しています。次にエンジニアは何を設定する必要がありますか？
A. セキュアファイアウォール脅威防御デバイスの侵入ポリシー
B. セキュアファイアウォール脅威防御デバイスのアクティブインターフェース
C. スイッチ上のDHCP
D. スイッチ上のアクティブなSPANポート
Answer: A (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスでトラフィックを検査し、IDSとして機能するIPSモードを設定するには、ネットワークエンジニアがFTDデバイスに侵入ポリシーを設定する必要があります。
スイッチのパッシブインターフェイスとSPANはすでに設定されており、トラフィックはFTDにミラーリングされます。
次のステップは、悪意のあるトラフィックを検出して対応するためのルールとアクションを定義する侵入ポリシーを設定することです。
手順:
* FMC で、[ポリシー] > [侵入] に移動します。
* 新しい侵入ポリシーを作成するか、既存の侵入ポリシーを編集します。
* 脅威を検出するためのルールとアクションを定義します。
* 侵入ポリシーを関連するインターフェースまたはアクセス制御ポリシーに適用します。
この設定により、FTD はミラーリングされたトラフィックを検査し、定義された侵入ポリシーに基づいて適切なアクションを実行できるようになります。
参考資料:Cisco Secure Firewall Management Center 管理者ガイド、侵入ポリシーの章。

最新問題**: 339**
管理対象デバイスをインラインで展開するための最小要件は何ですか?
A. インラインインターフェース、セキュリティゾーン、MTU、モード
B. パッシブインターフェース、MTU、モード
C. インラインインターフェース、MTU、モード
D. パッシブインターフェース、セキュリティゾーン、MTU、モード
Answer: C (メーッセージを残す**)**
セクション: 展開
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html

最新問題**: 340**
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ユーザーがランダムに切断されるという報告を受けています。ネットワーク監視ツールによると、FTDアプライアンスの使用率がピーク時に総容量の90%を超えています。この問題をさらに分析するには、どのような対策が必要ですか？
A. パケットエクスポート機能を使用してデータを外部ドライブに保存します

B. パケットキャプチャ機能を使用してリアルタイムのネットワークトラフィックを収集します
C. トラフィックポリシー分析にパケットトレーサー機能を使用する
D. ネットワークデータをキャプチャするためにパケット分析機能を使用する
Answer: B (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

最新問題**: 341**
Cisco Firepower 影響フラグの主な機能はどのオプションですか?
A. ASA が Firepower モジュールに送信するデータを識別します。
B. 侵入と脆弱性に関するデータを相関させます。
C. 重大なイベントが発生したときに管理者に警告します。
D. 既知の悪意のある IP アドレスと悪意のある疑いのある IP アドレスをレポートで強調表示します。
Answer: (解答を表示する**)**

最新問題**: 342**

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ます。リスクを軽減するために、エンジニアはどのような実装を推奨すべきでしょうか？
A. IPアドレスとURLのブラックリスト
B. 仮想保護
C. ネットワークベースの検出
D. トレンド分析
Answer: C (メーッセージを残す**)**

最新問題: **343**
ネットワーク管理者は、新しいCisco Secure Firewall Threat Defense（FTD）ファイアウォールを導入しようとしています。Cisco Secure FTDの導入後、内部クライアント間の接続が断続的に途切れるようになりました。管理者は、Secure FTDファイアウォールのパケットキャプチャで、Secure FIDが内部ネットワーク上のすべてのAW要求に応答していることを確認しました。この問題を解決するために、ネットワーク管理者はどのような対応を取るべきでしょうか？
A. NAT ポリシーを確認し、不正なプロキシ ARP 構成を無効にします。
B. FTD の MAC アドレスをクライアント マシンの IP マッピングにハードコードします。
C. アクセス ポリシーを確認し、内部から内部への ARP が許可されていることを確認します。
D. FTD を透過モードに変換して、ARP 要求を許可します。
Answer: A (メーッセージを残す**)**
内部クライアントで断続的な接続問題が発生しているにもかかわらず、Cisco Secure FTD が内部ネットワーク上のすべての ARP 要求に応答している場合、NAT ポリシーのプロキシ ARP 設定に誤りがある可能性があります。プロキシ ARP により、FTD が他のデバイスに代わって ARP 要求に応答し、接続の問題が発生する可能性があります。
解決手順:
* FTD の NAT ポリシーを確認し、不正なプロキシ ARP 設定を特定します。
* 問題の原因となっている関連する NAT ルールのプロキシ ARP 設定を無効にします。
これにより、FTD は必要に応じてのみ ARP 要求に応答するようになり、内部ネットワーク上の通常の ARP トラフィックに干渉することがなくなります。
参考資料: Cisco Secure Firewall Management Center 構成ガイド、NAT および ARP 構成の章。

最新問題: **344**
Cisco Firepower のインラインとインライン タップの違いは何ですか?
A. 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。
B. インライン タップ モードでは完全なパケット キャプチャが実行されます。
C. インライン モードでは悪意のあるトラフィックがドロップされる可能性があります。
D. インライン モードでは SSL 復号化は実行できません。
Answer: A (メーッセージを残す**)**

```
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
```

展示をご覧ください。ユーザーは様々なTCPポートで多数の外部リソースへの接続を試みています。ポート番号を間違えると、接続は即座に切断され、切断されるまでに1分以上かかります。エンジニアは、展示に示すように、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。
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には、エンジニアは何を構成する必要がありますか?
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ICMPタイプ3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TCPリセットパケットを許可する受信アクセスルール
Answer: C (メーッセージを残す**)**

最新問題: **346**
セキュリティエンジニアは、インターネットからのトラフィックを検査するためにCisco FTDアプライアンスを設定する必要があります。インターネットトラフィックはCisco Catalyst 9300スイッチからミラーリングされます。このタスクを実現するには、どの設定が必要ですか？
A. ファイアウォール モードをルーティングに設定します。
B. ファイアウォール モードを透過に設定します。
C. インターフェイス設定モードをなしに設定します。
D. インターフェイス設定モードをパッシブに設定します。
Answer: (解答を表示する**)**

最新問題: **347**
Cisco Secure Firewall Threat Defense デバイスでパケット キャプチャが使用され、パケット フローがマルウェア クエリを待機している場合、どの Snort 判定が表示されますか?
A. ブロック
B. 再試行
C. 置換
D. ブロックフロー
Answer: B (メーッセージを残す**)**
Cisco Secure Firewall Threat Defense（FTD）デバイスでパケットキャプチャが使用され、パケットフローがマルウェアクエリを待機している場合、Snortの判定は「再試行」と表示されます。これは、デバイスがマルウェア分析を処理中で、パケットに対する最終的なアクションをまだ決定していないことを示します。
「再試行」判定は、マルウェア検査の結果を待機している間、パケットが保留状態にあることを示し、最終的な決定が下されるまでセキュリティ態勢を維持するのに役立ちます。

最新問題: **348**
Cisco FMC 管理者は、パフォーマンスを向上させるために、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設定しますか?
A. アイデンティティポリシー
B. ネットワーク分析ポリシー
C. プレフィルターポリシー
D. 侵入ポリシー
Answer: C (メーッセージを残す**)**

最新問題: **349**
ネットワーク管理者は、アクティブ/パッシブの高可用性 Cisco FTD ペアを実装しています。
高可用性ペアを追加する場合、管理者はセカンダリ ピアを選択できません。
原因は何ですか？
A. 高可用性ペアを追加する前に、各 Cisco FTD でフェールオーバー リンクを定義する必要があります。
B. 高可用性ペアを追加する前に、高可用性ライセンスを Cisco FMC に追加する必要があります。
C. 2 番目の Cisco FTD は、プライマリ Cisco FTD と同じモデルではありません。
D. 両方のCisco FTDデバイスのソフトウェアバージョンが同じではありません
Answer: C (メーッセージを残す**)**

最新問題: **350**
Cisco AMP for Endpoints のどの 2 つの機能により、アップロードされたファイルをブロックできますか? (2 つ選択してください。)
A. アプリケーションのホワイトリスト
B. シンプルなカスタム検出
C. アプリケーションのブロック
D. 除外
E. ファイルリポジトリ
Answer: B,C (メーッセージを残す**)**

最新問題: **351**

パケットキャプチャにトレース オプションを選択する利点は何ですか?
A. このオプションは各パケットの詳細をキャプチャします。
B. このオプションは、パケットがドロップされたか成功したかを示します。
C. このオプションは、キャプチャされるパケットの数を制限します。
D. 宛先ホストが別のパスを介して応答するかどうかを示すオプション。
Answer: B (メーッセージを残す**)**

最新問題: **352**
エンジニアは、Cisco FTDデバイスとパブリックDNSサーバーの背後にあるエンドポイントからの接続問題を調査する必要があります。エンドポイントは名前解決クエリを実行できません。エンジニアは、Cisco FTD上で実際のDNSトラフィックをシミュレートしながらSnarl判定を検証することで、問題をトラブルシューティングするため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. FTD CLI から tcpdump を使用して Snort エンジンのキャプチャを実行します。
B. Cisco FMC の Capture w/Trace ウィザードを使用します。
C. Cisco FMC でカスタム ワークフローを作成します。
D. FTD CLI から system support firewall-engine-debug コマンドを実行します。
Answer: B (メーッセージを残す**)**
説明
Cisco FMCの 「Capture w/Trace」ウィザードを使用すると、FTDデバイス上のパケットをキャプチャし、Snortエンジンを介したパスをトレースできます。これにより、FTDデバイスとパブリックDNSサーバの背後にあるエンドポイントからの接続問題のトラブルシューティングや、DNSトラフィックに対するSnortの判定の検証が可能になります。 「Capture w/Trace」ウィザードでは、キャプチャおよびトレースするパケットの送信元と宛先のIPアドレス、ポート、プロトコル、およびキャプチャを実行するFTDデバイスとインターフェイスを指定できます。
フィルターを適用してキャプチャサイズと期間を制限することもできます。キャプチャを開始したら、エンドポイントからDNSサーバにpingを実行し、キャプチャされたパケットとそのSnort判定結果をFMC Web インターフェース2で確認できます。
Cisco FMC で Capture w/Trace ウィザードを使用するには、次の手順に従う必要があります2。
FMC Web インターフェイスで、[トラブルシューティング] > [キャプチャ/トレース] に移動します。
[新しいキャプチャ]をクリックします。
[デバイス] ドロップダウン リストから FTD デバイスを選択します。
「インターフェース」ドロップダウンリストからインターフェースを選択します。
キャプチャおよびトレースするパケットの送信元および宛先IPアドレス、ポート、プロトコルを入力します。例えば、IPアドレス10.1.1.100のエンドポイントからIPアドレス8.8.8.8のDNSサーバーへのDNSクエリをキャプチャする場合は、以下の値を入力します。
ソースIP: 10.1.1.100
送信元ポート: 任意
宛先IP: 8.8.8.8
宛先ポート: 53
プロトコル: UDP
必要に応じて、フィルターを適用してキャプチャサイズと期間を制限できます。たとえば、キャプチャするパケットの最大数、キャプチャファイルの最大サイズ、キャプチャ時間の最大時間などを設定できます。
[スタート]をクリックします。
エンドポイントから DNS サーバーに ping を実行し、いくつかのパケットがキャプチャされるのを待ちます。
キャプチャを停止するには、 「停止」をクリックします。
キャプチャされたパケットとその Snort 判定を表示するには、[キャプチャの表示] をクリックします。
その他のオプションは、次の理由により正しくありません。
FTD CLI から tcpdump を使用して Snort エンジンのキャプチャを実行しても、Snort エンジンを通過するパケットのパスを追跡したり、Snort の判定を確認したりすることはできません。tcpdump は FTD デバイス

上でパケットをキャプチャできるコマンドラインツールですが、Snort がパケットをどのように処理するか、またどのようなアクションを実行するかに関する情報は提供されません2。
Cisco FMCでカスタムワークフローを作成しても、FTDデバイスとパブリックDNSサーバの背後にあるエンドポイントからの接続問題のトラブルシューティングには役立ちません。カスタムワークフローは、イベントデータを表、グラフ、マップなど、様々な形式で表示するユーザ定義のページセットです。カスタムワークフローでは、FTDデバイス3上のパケットをキャプチャまたはトレースすることはできません。
FTD CLI から system support firewall-engine-debug コマンドを実行しても、FTD デバイス上の実際の DNS トラフィックをシミュレートしたり、そのトラフィックに対する Snort の判定を検証したりすることはできません。firewall-engine-debug コマンドは、合成パケットを生成し、FTD デバイスの Snort エンジンを介して送信できる診断ツールです。合成パケットは実際のネットワーク トラフィックではなく、FTD デバイス上の接続やポリシーに影響を与えません4。

最新問題: **353**
ネットワークセキュリティエンジニアは、高可用性ペア内の故障したCisco FTDデバイスを交換する必要があります。故障したユニットを交換する際には、どのようなアクションを実行する必要がありますか？
A. 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。
B. 障害のあるCisco FTDデバイスをCisco FMCから登録解除します。
C. 交換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. 交換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。
Answer: (解答を表示する)

最新問題: **354**
2 つの物理インターフェイスが名前付き BVI に割り当てられている場合、Cisco Secure Firewall Threat Defense はどのファイアウォール モードになりますか?
A. IPSのみ
B. ルーティング
C. 透明
D. インライン
Answer: C (メーッセージを残す)
BVI に割り当てられ、同じスイッチ上の異なる VLAN に接続された 2 つの物理インターフェイスが設定された Cisco FTD は、透過ファイアウォール モードをサポートするように設定されています。
透過モードでは、ファイアウォールはレイヤー2で動作し、通過するパケットのIPアドレスやMACアドレスを変更しません。このモードでは、ファイアウォールは両端のデバイスに対して透過的であり、IPアドレスやトポロジを変更することなくネットワークに挿入できます。
https://www.cisco.com/c/en/us/td/docs/security/cdo/cloud-delivered-firewall-management-center- in-cdo/managing-firewall-threat-defense-services-with-cisco-defense-orchestrator/m_device-ops- tfw.html

最新問題: **355**
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. coredump packet-engine 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
Answer: B (メーッセージを残す)
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/ac_1.html

最新問題: **356**
セキュリティエンジニアが複数のブランチ拠点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重要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ています。各拠点のポリシーの一貫性を維持しながら、適用可能なルールの範囲内でローカルで重要なネットワークサブネットのみを許可するには、どの手法が適切でしょうか？

A. ポリシー継承を利用する
B. 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
C. Cisco Talosから更新される動的なアクセス制御ポリシーを活用する
D. INSIDE_NET ネットワークオブジェクトとオブジェクトオーバーライドを使用してアクセス制御ポリシーを作成する
Answer: (解答を表示する**)**

最新問題**: 357**
エンジニアはCisco FMCのリモートストレージを設定する必要があります。災害復旧のため、設定のバックアップはネットワーク上の安全な場所から利用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、エンジニアはどのような戦略を採用すべきでしょうか？
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。
Answer: C (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/システム構成.html#ID-2241-00000551
バックアップを 1 つのリモート システムに送信し、レポートを別のリモート システムに送信することはできませんが、どちらかをリモート システムに送信し、もう 1 つを Firepower Management Center に保存することはできます。

最新問題**: 358**
エンジニアは新しい Firepower の展開を設定しており、実装を開始するためにデフォルトの FMC ポリシーを確認しています。組織は、最初の試用フェーズで、ネットワーク トラフィックの大部分を通過させながら、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。どのデフォルト ポリシーを使用する必要がありますか。
A. 最大検出
B. 接続性よりもセキュリティを重視
C. バランスの取れたセキュリティと接続性
D. セキュリティよりも接続性を重視
Answer: D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html

最新問題**: 359**
組織は、動作分析のために、Cisco FTD デバイスから Cisco Stealthwatch に NetFlow トラフィックを取り込むことができる必要があります。
この要件を満たすには、Cisco FTD で何を設定する必要がありますか?
A. NetFlow の flexconfig オブジェクト
B. NetFlowをエクスポートするためのインターフェースオブジェクト
C. NetFlow のセキュリティ インテリジェンス オブジェクト
D. NetFlowの変数セットオブジェクト
Answer: A (メーッセージを残す**)**
ステップ4. Netflowの宛先を設定する
Netflowの宛先を設定するには、「オブジェクト」> 「FlexConfig」> 「FlexConfigオブジェクト」に移動します。
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html#anc14

最新問題: **360**
エンジニアは、Cisco Secure Firewall Management Center を使用して管理されている IPSv デバイス上の NTP サーバを再設定する必要があります。エンジニアは、Secure Firewall Management Center と NTP サーバ間の安全な通信を検証しました。エンジニアは、Secure Firewall Management Center でどのように再設定を行う必要がありますか？
A. デバイス > プラットフォーム設定 > [割り当てられたセキュアファイアウォール設定ポリシー] > クラシック管理対象デバイス
B. デバイス > デバイス管理 > [NGIPSv デバイス] > デバイス > システム
C. デバイス > プラットフォーム設定 > [割り当てられた脅威防御設定ポリシー] > 時刻同期
D. デバイス > デバイス管理 > 時刻同期
Answer: (解答を表示する**)**

最新問題: **361**
あるエンジニアは現在、Cisco FMCに登録されたCisco FTDデバイスを所有しており、アドレス10 10.50.12が割り当てられています。組織ではアドレススキームのアップグレードを行っており、ネットワーク上で十分な数のアドレスを提供できる形式にアドレスを変換する必要があります。
新しいアドレス指定が有効になり、Cisco FTD から Cisco FMC への接続に使用できるようにするには、エンジニアは何をする必要がありますか?
A. デバイスを削除してCisco FMCに再登録します
B. Cisco FMCからデバイスを削除せずに、IPアドレスをIFV4からIPv6に更新します。
C. デバイスをフォーマットし、Cisco FMC に再登録します。
D. Cisco FMC は IPv4 IP アドレスを使用するデバイスをサポートしていません。
Answer: A (メーッセージを残す**)**
IPv4 を使用して FMC とデバイスを登録し、IPv6 に変換する場合は、デバイスを削除して再登録する必要があります。
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/device_management_basics.html

最新問題: **362**
エンジニアはCisco FMCのリモートストレージを設定する必要があります。災害復旧のため、設定のバックアップはネットワーク上の安全な場所から利用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、エンジニアはどのような戦略を採用すべきでしょうか？
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。
Answer: C (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/system
バックアップを 1 つのリモート システムに送信し、レポートを別のリモート システムに送信することはできませんが、どちらかをリモート システムに送信し、もう 1 つを Firepower Management Center に保存することはできます。

最新問題: **363**

Encrypted Visibility Engine (EVE) は、Cisco Secure Firewall Management Centre のアクセス制御ポリシーのどのラボで有効になっていますか?
A. ネットワーク分析ポリシー
B. 上級
C. セキュリティインテリジェンス
D. SSL
Answer: (解答を表示する**)**
Cisco Secure Firewall Management Center の Encrypted Visibility Engine（EVE）は、アクセス制御ポリシーの SSL タブで有効化できます。EVE は暗号化されたトラフィックを可視化し、トラフィックが暗号化されている場合でもファイアウォールが脅威を検出できるようにします。
EVE を有効にする手順:
* FMC のアクセス制御ポリシーに移動します。
* SSL タブに移動します。
* 暗号化されたトラフィックを分析するには、Encrypted Visibility Engine (EVE) を有効にします。
この構成は、完全な復号化を必要とせずに、暗号化されたトラフィック内の脅威を識別して軽減するのに役立ちます。
参考資料: Cisco Secure Firewall Management Center 構成ガイド、SSL および暗号化トラフィックの可視性に関する章。

最新問題**: 364**
Cisco FMC CLI ではどのコマンドライン モードがサポートされていますか?
A. 特権
B. ユーザー
C. 構成
D. 管理者
Answer: C (メーッセージを残す**)**
セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config- guide-v66/command_line_reference.pdf

最新問題**: 365**
ネットワークエンジニアは、侵入検知機能を活用するために、新しいCisco Firepowerデバイスをネットワークに実装しようとしています。デバイスを通過するトラフィックを分析し、悪意のあるトラフィックを警告し、Bump In Wire（BIP）として検出する要件があります。どのように実装すればよいでしょうか？
A. 接続されたデバイスのデフォルトゲートウェイとして BVI IP アドレスを指定します。
B. Cisco Firepowerでルーティングを有効にする
C. 物理的な Cisco Firepower インターフェイスに IP アドレスを追加します。
D. ブリッジ グループを透過モードで設定します。
Answer: D (メーッセージを残す**)**
従来、ファイアウォールはルーティングホップであり、遮蔽されたサブネットの1つに接続するホストのデフォルトゲートウェイとして機能します。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。ただし、他のファイアウォールと同様に、インターフェイス間のアクセス制御は制御され、通常のファイアウォールチェックはすべて実施されます。レイヤ2接続は、ネットワークの内部インターフェイスと外部インターフェイスをグループ化した「ブリッジグループ」を使用して実現されます。ASAはブリッジング技術を使用して、インターフェイス間のトラフィックを通過させます。各ブリッジグループには、ネットワーク上でIPアドレスを割り当てるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに対して複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互に通信できません。
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html

最新問題: **366**
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. システム生成すべてのトラブルシューティング
D. テクニカルサポートを表示
Answer: B (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

最新問題: **367**
展示品を参照してください。

既存の Cisco FMC 構成の効果は何ですか?
A. Cisco FMC と管理対象デバイス間の SSL 暗号化通信チャネルがプレーンテキスト通信チャネルになります。
B. Cisco FMC と Cisco FTD 間の管理接続が無効になっています。
C. Cisco FMC と管理対象デバイス間の通信用のリモート管理ポートがポート 8443 に変更されます。
D. 管理対象デバイスが Cisco FMC から削除されます。
Answer: B (メーッセージを残す**)**

最新問題: **368**
エンジニアは現在、Cisco FTDデバイスをCisco FMCに登録しており、アドレス10 10.50.12が割り当てられています。組織ではアドレス割り当てスキームをアップグレードしており、ネットワーク上で十分な数のアドレスを提供できる形式にアドレスを変換する必要があります。新しいアドレス割り当てが有効になり、Cisco FTDとCisco FMCの接続に使用できるようにするために、エンジニアはどのような対策を講じるべきでしょうか？
A. Cisco FMC は IPv4 IP アドレスを使用するデバイスをサポートしていません。
B. Cisco FMCからデバイスを削除せずに、IPアドレスをIFV4からIPv6に更新します。
C. デバイスを削除してCisco FMCに再登録します
D. デバイスをフォーマットし、Cisco FMC に再登録します。
Answer: (解答を表示する**)**

最新問題: **369**
展示品を参照してください。

展示を参照してください。エンジニアはアクセス制御ポーキーを変更して、ファイアウォールを通過するすべての DNS トラフィックを検査するルールを追加しています。変更を加えてポーキーを展開した後、DNS トラフィックが Snort エンジンによって完全に検査されていないことがわかりました。問題は何でしょうか。

A. ルールのアクションは、許可ではなく信頼に設定されています。
B. ルールは検査の送信元ネットワークとポートを定義する必要があります
C. ルールはトラフィックの発信元となるセキュリティゾーンを指定する必要があります
D. ルールの送信元ポートの設定が間違っています
Answer: A (メーッセージを残す)

最新問題**: 370**
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フィードを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で動作しており、メモリは8GBです。Threat 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. REST API アクセスを有効にします。
B. 7 GB のメモリを追加します。
C. バージョン 6.6 にアップグレードします。
D. TAXII サーバーを追加します。
E. TAXII サーバーの URL を追加します。
Answer: A,B (メーッセージを残す)

最新問題**: 371**
ドラッグアンドドロップの質問

添付資料を参照してください。エンジニアは、Cisco ASA 5500-XシリーズとCisco Secure Firewall Services Moduleを接続し、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設定する必要があります。フェイルオーバーを設定するには、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ください。すべてのオプションが使用されるわけではありません。

```
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.bbb7, MTU 1500
        Member GigabitEthernet1/5(Active), GigabitEthernet1/4
```

```
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	

Answer:

```
ASA(config)#interface Redundant1
ASA(config-if)# member-interface 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
```


GigabitEthernet1/5

backup interface GigabitEthernet1/4

reactivation mode timed

failover link Redundant1 GigabitEthernet1/4

Explanation:
ASA(config)# インターフェース Redundant1
ASA(config-if)# メンバーインターフェイス GigabitEthernet1/5
ASA(config-if)# メンバーインターフェイス GigabitEthernet1/4
redundant1コマンドは、プライマリインターフェースとセカンダリインターフェースをフェイルオーバーペアとして組み合わせる冗長インターフェースを作成します。その後、冗長インターフェース設定で各物理インターフェース（GigabitEthernet1/5およびGigabitEthernet1/4）のメンバーインターフェースを定義します。

最新問題: **372**
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-force-reset

B. システムサポートは ssl-client-hello が有効です
C. システムサポート ssl-client-hello-display
D. システムサポート ssl-client-hello-tuning
Answer: D (メーッセージを残す**)**

最新問題: **373**
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 が受信トラフィックと送信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. インターフェイスは自動ネゴシエーションを無効にし、インターフェイス速度は 1000 Mbps にハードコードされて設定されます。
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。
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01011010.html

最新問題: **374**
ネットワーク エンジニアは、別の IP サブネットを作成せずにトラフィック検査のために FTD デバイスを介してユーザー セグメントを拡張しています。これは、ルーティング モードの FTD デバイスでどのように実現されるのでしょうか。
A. ARPを利用してトラフィックをファイアウォールに誘導する
B. インラインセットインターフェースを割り当てることによって
C. BVIを使用して、ユーザーセグメントと同じサブネットにBVI IPアドレスを作成します。
D. 事前フィルタルールを活用してプロトコル検査をバイパスする
Answer: C (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

最新問題: **375**
Cisco Firepower Threat Defense では、ルーテッド インターフェイスを設定するときに、どの 2 つのインターフェイス設定が必要ですか? (2 つ選択してください。)
A. 冗長インターフェース
B. イーサチャネル
C. スピード
D. メディアタイプ
E. デュプレックス
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm-interfaces.html

最新問題: **376**
パケットキャプチャにトレース オプションを選択する利点は何ですか?
A. このオプションは、パケットがドロップされたか成功したかを示します。
B. このオプションは各パケットの詳細をキャプチャします。
C. 宛先ホストが別のパスを介して応答するかどうかを示すオプション。
D. このオプションは、キャプチャされるパケットの数を制限します。

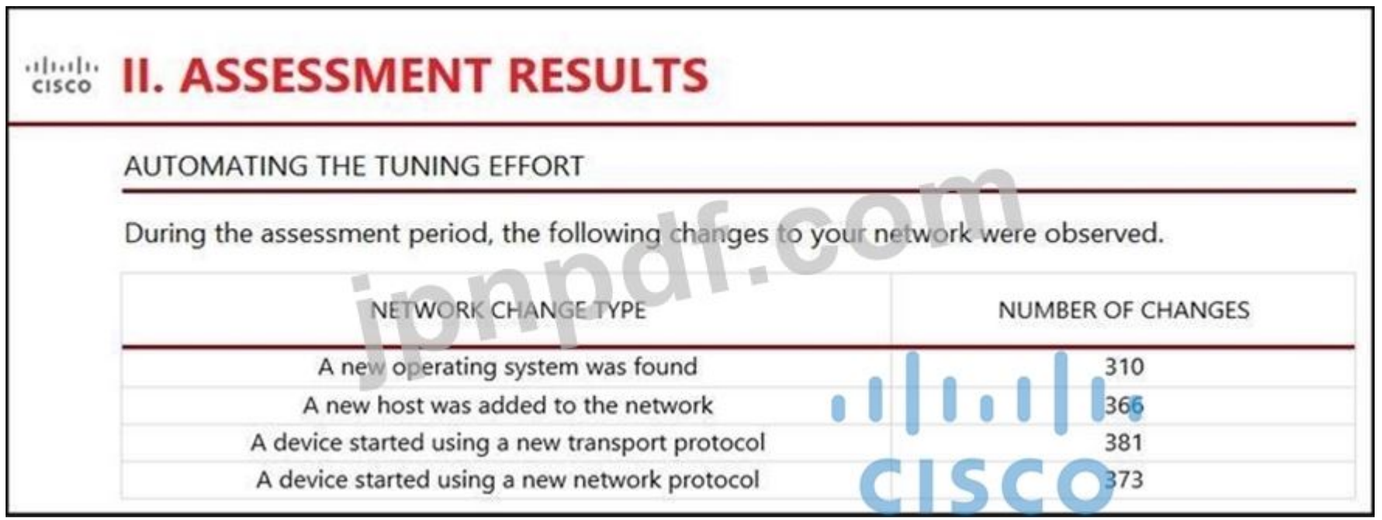
Answer: D (メーッセージを残す)

最新問題: **377**
Cisco 4100 シリーズ アプライアンスにインストールできるソフトウェアは何ですか? (2 つ選択してください)
A. だから
B. ASAv
C. FMC
D. FTD
Answer: (解答を表示する)

最新問題: **378**
Cisco FTD デバイスが透過ファイアウォール 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 タイプに IP アドレスを設定できますか (2 つ選択してください)。
A. BVI
B. 物理
C. イーサチャネル
D. 診断
E. サブインターフェース
Answer: A,D (メーッセージを残す)

最新問題: **379**
Cisco FMC データベース パージの動作は何ですか?
A. 適切なプロセスが再起動されます。
B. デバイスからデータを回復できます。
C. 指定されたデータは Cisco FMC から削除され、2 週間保持されます。
D. ユーザー アクティビティ チェック ボックスが選択されている場合、ユーザー ログインと履歴データはデータベースから削除されます。
Answer: A (メーッセージを残す)

最新問題: **380**
展示をご覧ください。エンジニアは攻撃リスクレポートを分析し、ネットワーク上で300件を超える新しいオペレーティングシステムのインスタンスが確認されていることを発見しました。
これらの新しいオペレーティング システムを保護するために、Firepower 構成はどのように更新されますか?



A. 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示します。
D. 管理者がポリシーを手動で更新します。
Answer: C (メーッセージを残す**)**
Firepower の IPS ポリシーの推奨事項は、ネットワーク検出と連携して IPS ポリシーに推奨事項を適用するツールですが、カスタム IPS ポリシーが自動的に推奨事項を取得するように設定しない限り、これを適用する必要があります (メモリ制限のため、1010 などのローエンド FW には推奨されません)。
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

最新問題: **381**
エンジニアは、既存のトランスペアレントなCisco FTDをルーテッドモードに変更したいと考えています。このデバイスは、2つのネットワークセグメント間のトラフィックを制御します。変更後、ホストがこれらの2つのセグメント間の通信を再確立できるようにするために必須のアクションはどれですか？
A. セグメント間のルーティングを行うために複数の BVI を設定します。
B. 各セグメントに重複しない IP サブネットを実装します。
C. 各ファイアウォール インターフェイスに一意の VLAN ID を割り当てます。
D. 既存の動的ルーティング プロトコル設定を削除します。
Answer: B (メーッセージを残す**)**

最新問題: **382**
エンジニアは、2 つの異なるネットワーク上にある営業部門と製品開発部門からのネットワーク トラフィックを監視しています。両部門のデータ プライバシーを維持するには、何を構成する必要がありますか?
A. トラフィックの分離を維持するために、各部門に専用のIPSインラインセットを使用します。
B. 両部門でTAPモードでインラインセットのペアを1つ使用します。
C. 論理トラフィック分離を維持するために、VLANで802 1Q MIMEセットトランクインターフェースを使用する
D. 両部門でパッシブIDSポートを使用する
Answer: (解答を表示する**)**
最新問題: **383**

エンジニアは、Cisco Secure Firewall Management Center を使用して Cisco Secure Firewall Threat Defense デバイスのパケットキャプチャ機能にアクセスし、接続の問題を調査する必要があります。エンジニアは、Secure Firewall Threat Defense デバイスを通過する実際のパケットと Snort 検出アクションを確認する必要があります。パケットキャプチャを確認しているときに、エンジニアは Snort 検出アクションが欠落していることに気付きました。この問題を解決するために、エンジニアはどのような措置を講じるべきでしょうか。
A. バッファサイズを指定します。
B. 連続キャプチャオプションを有効にします。
C. トレース オプションを有効にします。
D. パケット サイズを指定します。
Answer: (解答を表示する**)**

最新問題**: 384**
管理者は、Firepower をしばらく使用し、Firepower がネットワークとどのように相互作用するかを学習した後、悪意のあるアクティビティとユーザーを関連付けようとしています。
Cisco Firepower ダッシュボードでこの可視性を実現するには、どのウィジェットを設定する必要がありますか?
A. カスタム分析
B. 現在のステータス
C. 現在のセッション
D. 相関イベント
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/dashboards.html#ID-2206-00000283

最新問題**: 385**
Syslog を使用するのではなく、Cisco Firepower 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直接 Cisco Threat Response にイベントを送信する利点は何ですか?
A. Firepower 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。
B. すべてのタイプの Firepower デバイスがサポートされています。
C. サポートされているバージョンの Firepower を実行しているすべてのデバイスをサポートします。
D. オンプレミスのプロキシサーバーはセットアップやメンテナンスの必要がない
Answer: (解答を表示する**)**
参照：
Firepower と Cisco 脅威対応の統合ガイド.pdf

最新問題**: 386**
エンジニアは、Cisco Secure Firewall Management Center を使用して、Cisco Secure IPS に ERSPAN パッシブインターフェースを設定する必要があります。以下の設定はすでに実行済みです。
- パッシブ インターフェイスを構成します。
- ERSPAN IP アドレスを設定します。
構成を完了するには、どの 2 つの追加設定を構成する必要がありますか? (2 つ選択してください。)
A. 宛先MAC
B. TCPインターセプト
C. バイパスモード
D. フローID
E. 送信元IP
Answer: A,D (メーッセージを残す**)**

Cisco Secure Firewall Management Center を使用して Cisco Secure IPS 上の ERSPAN パッシブ インターフェイスの設定を完了するには、次の追加設定が必要です。
- 宛先 MAC: ERSPAN トラフィックの宛先を識別するために必要です。
- フロー ID: ERSPAN セッションを一意に識別します。これは、ミラーリングされたトラフィックを正しく処理するために不可欠です。

最新問題: **387**
ネットワークエンジニアは、侵入検知機能を活用するために、新しいCisco Firepowerデバイスをネットワークに実装しようとしています。デバイスを通過するトラフィックを分析し、悪意のあるトラフィックを警告し、Bump In Wire（BIP）として検出する要件があります。どのように実装すればよいでしょうか？
A. 接続されたデバイスのデフォルトゲートウェイとして BVI IP アドレスを指定します。
B. Cisco Firepowerでルーティングを有効にする
C. 物理的な Cisco Firepower インターフェイスに IP アドレスを追加します。
D. ブリッジ グループを透過モードで設定します。
Answer: D (メーッセージを残す**)**
従来、ファイアウォールはルーティングホップであり、遮蔽されたサブネットのいずれかに接続するホストのデフォルトゲートウェイとして機能します。一方、透過型ファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤー2ファイアウォールであり、接続されたデバイスへのルーターホップとしては認識されません。ただし、他のファイアウォールと同様に、インターフェース間のアクセス制御は制御されており、通常のファイアウォールチェックはすべて実施されます。
レイヤ2接続は、「ブリッジグループ」を使用することで実現されます。ブリッジグループでは、ネットワークの内部インターフェイスと外部インターフェイスをグループ化し、ASAはブリッジング技術を使用してインターフェイス間のトラフィックを通過させます。各ブリッジグループには、ネットワーク上でIPアドレスを割り当てるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互に通信できません。https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html

最新問題: **388**
レポート テンプレートを作成するときに、特定のサブネットのアクティビティのみを表示するように結果を制限するにはどうすればよいですか?
A. 検索フィールドが CIDR 形式のネットワークとして定義されたレポートにテーブル ビュー セクションを追加します。
B. レポートの詳細設定で入力パラメータを追加し、タイプをネットワーク/IP に設定します。
C. Firepower Management Center でカスタム検索を作成し、レポートの各セクションで選択します。
D. レポートの各セクションで、X 軸として IP アドレスを選択します。
Answer: B (メーッセージを残す**)**

最新問題: **389**
ネットワーク管理者は、要求されたURL検索に基づいて悪意のあるサイトをブロックするデフォルトポリシーを設定したいと考えています。この要件を満たす機能はどれですか？
A. ファイルポリシー
B. マルウェアポリシー
C. URLフィルタリングポリシー
D. DNSポリシー
Answer: (解答を表示する**)**

最新問題: **390**
管理者はネットワークをより適切にセグメント化するためにインターフェースオブジェクトを作成しようとしていますが、オブジェクトにインターフェースを追加する際に問題が発生しています。この失敗の原因は何ですか？
A. インターフェースは複数のインターフェース グループに属しています。

B. 管理者は複数のゾーンにあるインターフェースを追加しています。
C. インターフェースは複数のネットワークの NAT に使用されています。
D. 管理者は複数のタイプのインターフェースを追加しています。
Answer: (解答を表示する**)**

最新問題: **391**
展示品を参照してください。

エンジニアがCisco Secure Firewall Management Center（FMC）でトラブルシューティングファイルを生成します。ファイルがダウンロードされる前に、正常に完了したタスクが削除されます。ファイル名を特定し、生成されたトラブルシューティングファイルを再生成せずに取得するには、どの2つの操作を実行する必要がありますか？（2つ選択してください。）
A. Secure FMC の FTP クライアント Hi エキスパート モードを使用して、ファイルを FTP サーバーにアップロードします。
B. 図に示されているのと同じ画面に移動し、「高度なトラブルシューティング」をクリックし、ファイル名を入力してダウンロードを開始します。
C. FTD67 および FTD66 デバイスの CU に接続し、フラッシュから PIP サーバーにタイルをコピーします。
D. Secure FMCのエキスパートモードに移行します。/Var/commonの内容を一覧表示し、出力から正しいファイル名を決定します。
E. [システム監視]、[監査] の順にクリックし、[トラブルシューティング ファイルの生成] 文字列を含む行から正しいファイル名を決定します。
Answer: (解答を表示する**)**
Cisco Secure Firewall Management Center (FMC) でトラブルシューティング ファイルを生成するタスクが正常に完了したが、ファイルがダウンロードされる前に削除された場合は、次の手順を実行してファイル名を決定し、生成されたトラブルシューティング ファイルを再生成せずに取得できます。
Secure FMC のエキスパート モードに移動します。
SSH またはコンソール経由で FMC のエキスパート モードにアクセスします。
生成されたトラブルシューティングファイルを見つけるには、/var/commonディレクトリの内容を一覧表示します。ls /var/commonコマンドを使用してください。
システム監視監査ログを使用します。
FMC で、[システム] > [監視] > [監査] に移動します。
「Generate Troubleshooting Files」という文字列を含む行を見つけて、正しいファイル名を確認します。
これらのアクションにより、生成されたトラブルシューティング ファイルを再生成する必要なく識別して取得できるため、時間とリソースを節約できます。
参考資料:Cisco Secure Firewall Management Center 管理者ガイド、トラブルシューティングとファイル管理の章。

最新問題: **392**

ある組織では、インターネットに接続するリンクで大量のトラフィックの混雑が発生していることに気づきました。
企業を離れる前にインターネットに送信されるすべてのトラフィックを処理する Cisco Firepower デバイスがあります。
正当なビジネストラフィックが目的地に到着するように、混雑をどのように緩和しますか?
A. 高帯域幅アプリケーションのレートを制限するQoSポリシーを作成する
B. アプリケーション対応帯域幅制限にWCCPを使用するためのflexconfigポリシーを作成します。
C. Cisco Firepowerデバイスが多くのアドレスを変換する必要がないようにNATポリシーを作成します。
D. ビジネスアプリケーションへの直接トンネルが確立されるようにVPNポリシーを作成します。
Answer: (解答を表示する**)**

最新問題: **393**
複数のドメインが使用されているマルチテナント展開では、グローバル ドメインの外部にどの更新を適用する必要がありますか?
A. メジャーアップグレードのローカルインポート
B. 侵入ルールのローカルインポート
C. Cisco 地理位置情報データベース
D. マイナーアップグレード
Answer: C (メーッセージを残す**)**

最新問題: **394**
ある企業は、2台のCisco FTDデバイスの容量を集約し、帯域幅や1秒あたりの接続数などのリソースを最大限に活用するソリューションを求めています。この要件を満たすには、Cisco FTDとCisco FMCを連携させて、どのような手順で処理を実行する必要がありますか？
A. Cisco FTD インターフェイスを設定し、FMC にメンバーを追加し、FMC でクラスタ メンバーを設定し、Cisco FMC でクラスタを作成します。
B. Cisco FTD インターフェイスとクラスタ メンバーを設定し、Cisco FMC にメンバーを追加します。そして、Cisco FMC でクラスタを作成します。
C. Cisco FMC にメンバーを追加し、Cisco FMC で Cisco FTD インターフェイスを設定します。Cisco FMC でクラスタ メンバーを設定し、Cisco FMC でクラスタを作成します。Cisco FMC でクラスタ メンバーを設定します。
D. Cisco FMC にメンバーを追加し、Cisco FTD インターフェイスを設定し、Cisco FMC でクラスタを作成し、Cisco FMC でクラスタ メンバーを設定します。
Answer: D (メーッセージを残す**)**

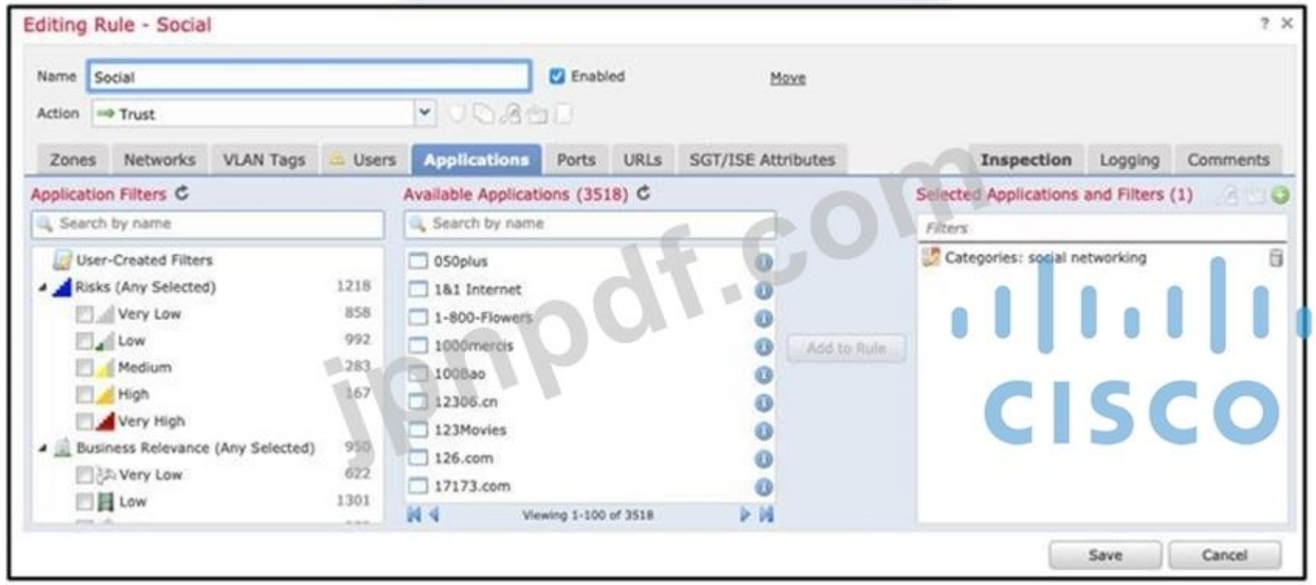
最新問題: **395**
エンジニアがHTTPトラフィック用のカスタムアプリケーション検出器を設定しており、サードパーティから提供されたファイルをインポートしたいと考えています。高度なアプリケーション検出器はどのような種類のファイルを作成し、アップロードしますか？
A. NBARプロトコル
B. Perlスクリプト
C. TAKEスクリプト
D. Pythonプログラム
Answer: C (メーッセージを残す**)**

最新問題: **396**
管理者は、インラインIPS展開におけるCisco Secure Firewall Threat Defenceデバイスのインターフェースを設定します。管理者は以下の操作を実行します。
* デバイスとインターフェースを識別します
* インターフェースモードをインラインに設定する
* インターレースを有効にする

実装を完了するために管理者が次に実行する必要がある構成手順は何ですか?
A. インターフェイスでスパニングツリー PortFast を有効にします。
B. インラインセットを構成する
C. インターフェースを透過モードに設定します。
D. インターフェイスをルーティング モードに設定します。
Answer: (解答を表示する**)**
インラインIPS環境において、Cisco Secure Firewall Threat Defense（FTD）デバイスのインターフェイスモードをインラインに設定し、インターフェイスを有効にした後、インラインセットを設定します。インラインセットは、2つのインターフェイスをグループ化し、それらの間を通過するトラフィックを検査するために連携して動作します。
インライン セットを構成する手順:
* FMC で、[デバイス] > [デバイス管理] に移動します。
* FTD デバイスを選択し、インターフェイスを設定します。
* インライン モードに設定されている関連インターフェイスを追加して、新しいインライン セットを作成します。
* 設定を FTD デバイスに展開します。
インライン セットを設定すると、指定されたインターフェイス間のトラフィックが IPS ポリシーに従って検査および処理され、インライン IPS 展開の実装が完了します。
参考資料: Cisco Secure Firewall Management Center 構成ガイド、インライン セットの章。

最新問題**: 397**
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. sudo sf_troubleshoot.pl
B. テクニカルサポートを表示
C. システム生成すべてのトラブルシューティング
D. システムサポートビューファイル
Answer: C (メーッセージを残す**)**

最新問題**: 398**
展示品を参照してください。



組織には、すべてのソーシャル メディア トラフィックを検査用に送信することを目的としたアクセス制御ルールがあります。しばらくルールを使用した後、管理者はトラフィックが検査されずに自動的に許可されていることに気付きました。この問題を解決するには、何をする必要がありますか?

A. ソーシャルネットワークのURLをブロックリストに追加する

B. ルール内で選択したアプリケーションを変更します

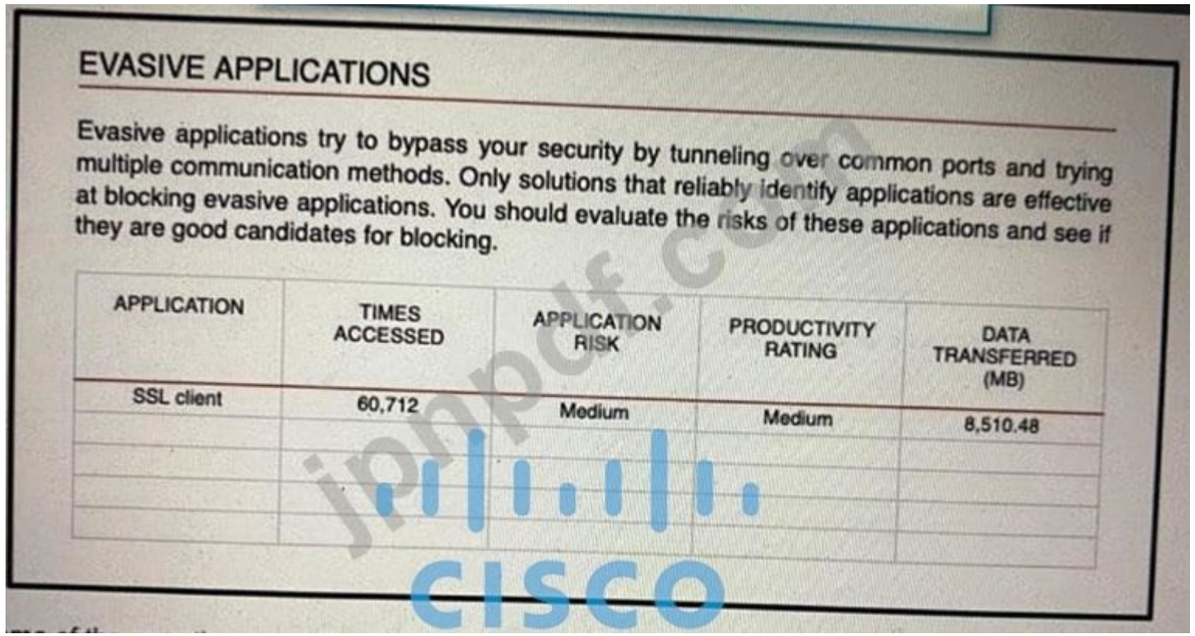
C. 侵入ポリシーをセキュリティよりも接続性重視に変更します。

D. ルールアクションを信頼から許可に変更します

Answer: (解答を表示する**)**

最新問題: **399**

展示品を参照してください。



管理者がCisco Firepowerのレポート機能を確認していたところ、ネットワークリスクレポートのこのセクションに、回避に利用される可能性のあるSSLアクティビティが多数表示されていることに気づきました。
このリスクを軽減するには、どのような対策を講じればよいでしょうか？
A. Cisco AMP for Endpoints を使用してすべての SSL 接続をブロックします
B. SSL 復号化を使用してパケットを分析します。
C. 暗号化されたトラフィック分析を使用して攻撃を検出する
D. Cisco Tetration を使用して、サーバへの SSL 接続を追跡します。
Answer: B (メーッセージを残す**)**

最新問題: **400**
エンジニアは、Cisco FMC で URL オブジェクトを定義する必要があります。
SSL 検査を実行せずに 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. オブジェクト内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。
Answer: (解答を表示する**)**
HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。
HTTPS URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-access.html

最新問題: **401**
ある組織では、Cisco FTDとCisco ISEを使用してアイデンティティベースのアクセス制御を行っています。ネットワーク管理者がCisco FTDのイベントを分析したところ、未知のユーザートラフィックがファイアウォールを通過できていることに気付きました。正当なユーザートラフィックを許可しながら、このトラフィックをブロックするには、どのように対処すればよいでしょうか？

A. Cisco ISE 許可ポリシーを変更して、ユーザへのこのアクセスを拒否します。
B. 正当なユーザー名のみを Cisco FTD に送信するように Cisco ISE を変更します。
C. Cisco FTD のアクセス コントロール ポリシーに不明なユーザーを追加します。
D. Cisco FTD のマルウェアおよびファイル ポリシーに不明なユーザーを追加します。
Answer: C (メーッセージを残す**)**
参考:https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd- fdm-identity.html#concept_655B055575E04CA49B10186DEBDA301A

最新問題**: 402**
展示を参照してください。他のすべてのウェブサイトへの同様の通信を防ぎながら、このウェブサイトへのアクセスを修正するには、何をする必要がありますか？
A. Snort がポート 80 を 172.1.1.50 のみに許可するように侵入ポリシー ルールを作成します。
B. Snort がポート 443 を 172.1.1.50 のみに許可するように侵入ポリシー ルールを作成します。
C. ポート 443 を 172.1.1.50 のみに許可するアクセス制御ポリシー ルールを作成します。
D. ポート 80 を 172.1.1.50 のみに許可するアクセス制御ポリシー ルールを作成します。
Answer: (解答を表示する**)**

最新問題**: 403**
ユーザーがブリッジをルーテッド モードで設定し、デバイスがインターフェイス間でレイヤ 2 スイッチングを実行できるようにする Firepower 機能はどれですか。
A. BDI
B. IRB
C. 軍曹
D. フレックスコンフィグ
Answer: (解答を表示する**)**

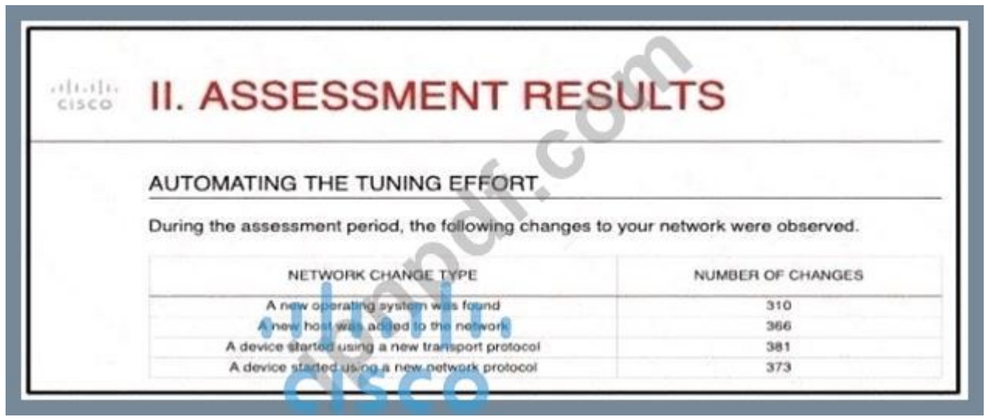
最新問題**: 404**
エンジニアは、Cisco FMCを使用して、ネットワーク経由で送信されるファイルがマルウェアであるかどうかを判断するという任務を負っています。このファイル検索を実行するには、どの2つの設定タスクを実行する必要がありますか？ 2つ選択してください。）
A. Cisco FMC には SSL 復号化ポリシーが含まれている必要があります。
B. Cisco FMC は Cisco AMP for Endpoints サービスに接続する必要があります。
C. サンドボックス化のために、Cisco FMC は Cisco ThreatGrid サービスに直接接続する必要があります。
D. Cisco FMC は FireAMP クラウドに接続する必要があります。
E. Cisco FMC には、マルウェア検索用のファイル検査ポリシーが含まれている必要があります。
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#ID-2193-00000296

最新問題**: 405**
エンジニアは、サードパーティ製のセキュリティインテリジェンスツールを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で動作しており、メモリは8GB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サーバーを追加する
Answer: (解答を表示する**)**
Threat Intelligence Director (TID) を使用してサードパーティのセキュリティ インテリジェンス フィードを Cisco Secure Firewall Management Center (FMC) と統合するには、次のアクションが必要です。
* バージョン 6.6 へのアップグレード: Threat Intelligence Director をサポートするには、FMC が少なくともバージョン 6.6 を実行している必要があります。バージョン 6.2.3 では、この統合に必要な機能がサポートされていません。
* TAXIIサーバのURLを追加 :Threat Intelligence Directorは、TAXII（Trusted Automated eXchange of Indicator Information）を使用してサードパーティソースから脅威インテリジェンスデータを取得します。TAXIIサーバのURLをFMCのTID設定に追加する必要があります。
手順:
* FMC をバージョン 6.6 以降にアップグレードします。
* FMC で、[統合] > [脅威インテリジェンス ディレクター] に移動します。
* TAXII サーバーの URL を入力して、新しい TAXII サーバーを追加します。
これらのアクションにより、サードパーティの脅威インテリジェンス フィードとの統合が可能になり、FMC のセキュリティ機能が強化されます。
参考資料: Cisco Secure Firewall Management Center 管理者ガイド、Threat Intelligence Director の章。

最新問題**: 406**
病院ネットワークでは、Cisco FMC管理対象デバイスのアップグレードと、災害復旧プロセスの確実な実施が求められています。ネットワークのダウンタイムを最小限に抑えるには、何をすべきでしょうか？
A. 冗長性を高めるためにISPへの2番目の回線を構成する
B. バックアップとして使用するために現在の構成のコピーを保持します
C. フェイルオーバー用にCisco FMCを設定する
D. Cisco FMC 管理対象デバイスをクラスタリング用に設定します。
Answer: (解答を表示する**)**
Cisco Threat Intelligence Director（TID）と高可用性構成 高可用性構成において、アクティブなFirepower Management CenterでTIDをホストする場合、システムはTID構成とTIDデータをスタンバイFirepower Management Centerに同期しません。フェイルオーバー後にデータを復元できるように、アクティブなFirepower Management CenterでTIDデータを定期的にバックアップすることをお勧めします。
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/firepower_management_center_high_availability.html

最新問題**: 407**
展示品を参照してください。



エンジニアは攻撃リスク レポートを分析し、ネットワーク上で 300 を超える新しいオペレーティング システムのインスタンスが確認されていることを発見しました。これらの新しいオペレーティング システムを保護するために、Firepower 構成はどのように更新されるのでしょうか。

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示します。
D. 管理者がポリシーを手動で更新します。
Answer: C (メーッセージを残す**)**
参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60
/ネットワーク資産への侵入防御のカスタマイズ.html

最新問題: **408**
インライン セット プロパティの [詳細設定] タブでは、どの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ますか?
A. 透過インラインモード
B. 厳密なTCP強制
C. リンク状態を伝播する
D. TAPモード
Answer: C (メーッセージを残す**)**

最新問題: **409**
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. coredump packet-engine 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
Answer: C (メーッセージを残す**)**
SNORTエンジンのキャプチャには「capture-traffic」コマンドを使用します。LINAエンジンのキャプチャには「capture」コマンドを使用します。LINAエンジンはデバイスの実際の物理インターフェースを表すため、「capture」が唯一の合理的な選択肢です。参考 :https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working- with-firepower-threat-defense-f.html#anc10

最新問題: **410**

ネットワークエンジニアは、アクティブ/スタンバイ構成の物理Cisco Secure Firewall ASAペアを、Cisco Secure Firewall Threat Defense仮想アプライアンスペアに置き換えることを計画しています。現在の高可用性構成をサポートする仮想環境は2つありますか？ 2つ選択してください。）
A. ESXi
B. アズール
C. OpenStack
D. KVM
E. AWS
Answer: A,D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

最新問題: **411**
脅威対応チームは、脅威の分析と調査にシスコ社内のどのグループを使用していますか?
A. シスコ ディープ アナリティクス
B. OpenDNS グループ
C. シスコネットワークレスポンス
D. シスコ タロス
Answer: D (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

最新問題: **412**
Cisco AMP for Networks の展開において、クラウドに到達できない場合、どのような処理が返されますか?
A. 利用できません
B. 不明
C. クリーン
D. 切断されました
Answer: (解答を表示する**)**
利用不可は、システムが AMP クラウドを照会できなかったことを示します。
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_malware_events_and_network_file_trajectory.html

最新問題: **413**
エンジニアがFTD導入環境におけるアプリケーション障害のトラブルシューティングを行っています。FMC CLIを使用している際に、問題のトラフィックが適切なポリシーと一致していないことが判明しました。これを修正するにはどうすればよいでしょうか？
A. system support firewall-engine-dump-user-f density-data コマンドを使用してポリシーを変更し、アプリケーションがファイアウォールを通過できるようにします。
B. system support firewall-engine-debug コマンドを使用して、トラフィックがどのルールに一致しているかを判断し、それに応じてルールを変更します。
C. system support application-identification-debug コマンドを使用して、トラフィックがどのルールに一致しているかを判断し、それに応じてルールを変更します。
D. システム サポート ネットワーク オプション コマンドを使用して、ポリシーを微調整します。
Answer: B (メーッセージを残す**)**

最新問題: **414**

トラブルシューティング ファイルを生成するには、Cisco FMC CLI でどのコマンドを入力しますか?
A. 実行中の設定を表示
B. テクニカルサポートシャーシの表示
C. システムサポート診断 CLI
D. sudo sf_troubleshoot.pl
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

最新問題**: 415**
ネットワークエンジニアは、侵入検知機能を活用するために、新しいCisco Firepowerデバイスをネットワークに実装しようとしています。デバイスを通過するトラフィックを分析し、悪意のあるトラフィックを警告し、Bump In Wire（BIP）として検出する要件があります。どのように実装すればよいでしょうか？
A. 接続されたデバイスのデフォルトゲートウェイとして BVI IP アドレスを指定します。
B. Cisco Firepowerでルーティングを有効にする
C. 物理的な Cisco Firepower インターフェイスに IP アドレスを追加します。
D. ブリッジ グループを透過モードで設定します。
Answer: (解答を表示する**)**
従来、ファイアウォールはルーティングホップであり、そのサブネットに接続するホストのデフォルトゲートウェイとして機能します。一方、透過型ファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。ただし、他のファイアウォールと同様に、インターフェース間のアクセス制御は制御されており、通常のファイアウォールチェックはすべて実施されます。レイヤ
2 接続は、「ブリッジグループ」を使用することで実現されます。ブリッジグループでは、ネットワークの内部インターフェイスと外部インターフェイスをグループ化し、ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通過させます。各ブリッジグループには、ネットワーク上で IP アドレスを割り当てるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互に通信できません。
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.h

最新問題**: 416**
図を参照してください。Cisco Secure Firewall Threat Defense（FTD）デバイスが、インラインセットを使用してインラインモードで導入されています。ネットワークエンジニアは、ルーティング先のルータR1とセキュアFTDデバイス間のケーブルが切断された場合、ルータR2が直接接続されているルート192.168.1.0/24をルーティングテーブルから削除するようにしたいと考えています。エンジニアはどのようなアクションを実行する必要がありますか？

A. Secure FTDデバイスにリンクの古さを伝播するオプションを実装する
B. R1 と R2 の間にルーティング プロトコルを確立します。
C. Secure FTD デバイス上のハードウェア バイパスを無効にします。

D. R2のGi0/2インターフェースに自動ステート機能を実装する
Answer: A (メーッセージを残す**)**
ルータR1とSecure FTDデバイス間のケーブルが切断された際に、ルータR2が192.168.1.0/24への直接接続ルートをルーティングテーブルから削除するようにするには、ネットワークエンジニアがSecure FTDデバイスに 『リンク状態を伝播』オプションを実装する必要があります。このオプションにより、FTDはリンク状態の変化を隣接デバイスに伝播し、切断が認識され、それに応じてルーティングテーブルが更新されます。
手順:
FMC 経由で FTD デバイス構成にアクセスします。
関連するインターフェースのインターフェース設定に移動します。
R1 および R2 に接続されているインターフェースに対して 『リンク状態の伝播』オプションを有効にします。
変更を FTD デバイスに展開します。
この設定により、リンク状態の変更がルータ R2 に伝達され、切断されたルートをルーティング テーブルから削除するように要求されます。

最新問題: **417**
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。Cisco FTD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、トラフィックが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どうすればよいでしょうか？
A. 影響を受けるデバイスを再起動して設定をリセットします
B. 影響を受けるデバイスに構成を再展開して、SIモジュールに追加のメモリが割り当てられるようにします。
C. 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に交換します。
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
Answer: B (メーッセージを残す**)**

最新問題: **418**
エンジニアは、Cisco FMC のパケット キャプチャ ツールを使用して、Web サーバーへの HTTP トラフィックのトラブルシューティングを行っています。
エンジニアはキャプチャを確認したところ、キャプチャ対象のWebサーバーから送信されたパケットや、Webサーバー宛てのパケットが多数あることに気づきました。Cisco FTDデバイスで無関係なトラフィックのパケットをキャプチャする負担を軽減するにはどうすればよいでしょうか？
A. パケット キャプチャ出力を、Wireshark で開くことができる .pcap ファイルにリダイレクトします。
B. パケット キャプチャでホスト フィルターを使用して、特定のホストとの間のトラフィックをキャプチャします。
C. -c オプションを使用して、パケット キャプチャを最初の 100 パケットのみに制限します。
D. パケット キャプチャ内のアクセス リストを使用して、Web サーバーとの間の HTTP トラフィックのみを許可します。
Answer: (解答を表示する**)**

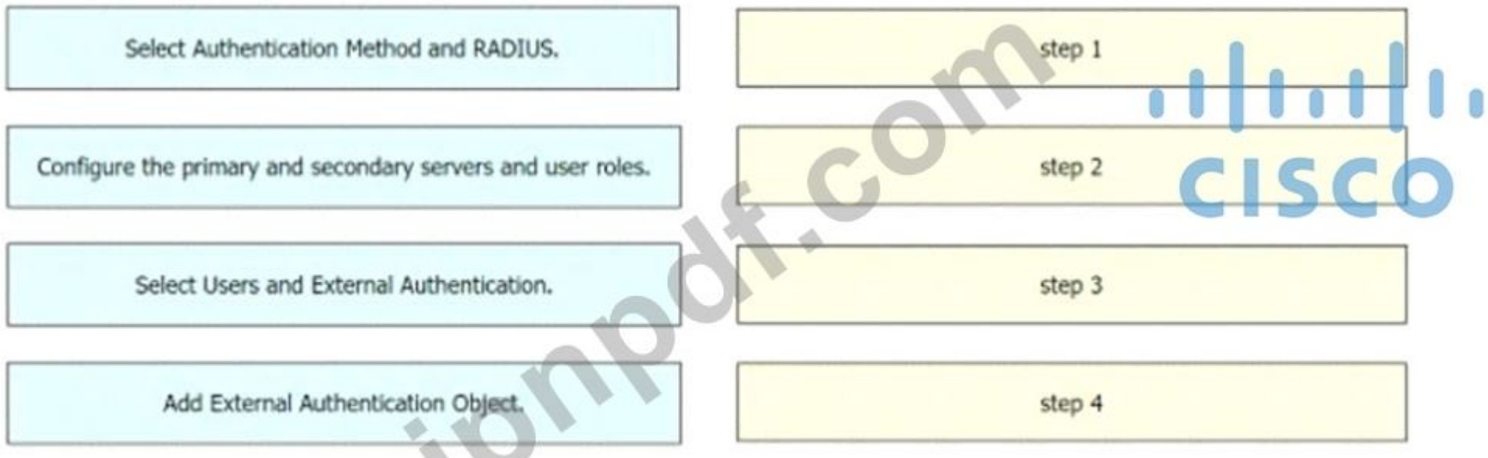
最新問題: **419**
ある企業は、Cisco FMCで管理されている複数のCisco FTDアプライアンスに侵入防御を導入しています。速度と検出を優先する場合、どのシステム標準ポリシーを選択する必要がありますか？
A. 接続性よりもセキュリティを重視
B. 最大検出
C. セキュリティよりも接続性を重視
D. バランスの取れたセキュリティと接続性
Answer: D (メーッセージを残す**)**

最新問題: **420**
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使用して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 アドレスを指定するタスクを担当

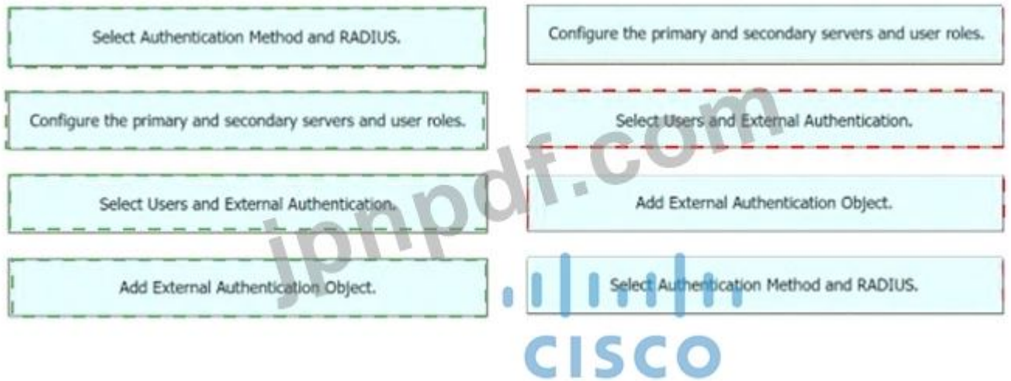
するエンジニアが考慮する必要があることは何ですか。
A. VLAN ID値が入力されている場合、宛先MACアドレスはオプションです。
B. UDPパケットタイプのみがサポートされています
C. パケットログの出力形式オプションは利用できません
D. VLAN IDと宛先MACアドレスはオプションです
Answer: A (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

最新問題**: 421**
エンジニアは、2 つの異なるネットワーク上にある営業部門と製品開発部門からのネットワーク トラフィックを監視しています。
両部門のデータのプライバシーを維持するために何を設定する必要がありますか?
A. トラフィックの分離を維持するために、各部門に専用のIPSインラインセットを使用します。
B. 論理トラフィック分離を維持するために、VLANで802.1Q MIMEセットトランクインターフェースを使用する
C. 両部門でパッシブIDSポートを使用する
D. 両部門でTAPモードでインラインセットのペアを1つ使用します。
Answer: A (メーッセージを残す**)**
インライン セットおよびパッシブ インターフェイスは、物理インターフェイスと EtherChannel のみをサポートし、冗長インターフェイスや VLAN などは使用できません。Firepower 4100/9300 サブインターフェイスも、IPS 専用インターフェイスではサポートされません。
インライン セットおよびパッシブ インターフェイスの場合、FTD はパケット内で最大 2 つの 802.1Q ヘッダーをサポートします (Q-in-Q サポートとも呼ばれます)。ただし、Firepower 4100/9300 は例外で、1 つの 802.1Q ヘッダーのみをサポートします。
注: ファイアウォール タイプのインターフェイスは Q-in-Q をサポートせず、1 つの 802.1Q ヘッダーのみをサポートします。

最新問題**: 422**
左側の設定手順を右側のシーケンスにドラッグ アンド ドロップして、Cisco FMC で RADIUS サーバーへの外部認証を有効にします。



Answer:



説明

4、1、2、3

最新問題: **423**

FlexConfig を使用せずに Firepower Threat Defense でサポートされる動的ルーティング プロトコルはどれですか (2 つ選択してください)。

A. EIGRP

B. OSPF

C. 静的ルーティング

D. IS-IS

E. BGP

Answer: (解答を表示する**)**

参照：

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

最新問題: **424**

ネットワーク管理者は、Cisco FTD によって検出されたファイルについて 不明」と判定されたことを確認しています。Talos クラウドで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設定オプションを選択する必要がありますか？
A. スペロ分析
B. マルウェア分析
C. 動的解析
D. サンドボックス分析
Answer: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html

最新問題**: 425**
エンジニアがCisco FMCを使用して新しいアクセス制御ポリシーを構築しています。このポリシーでは、固有のIPSポリシーとログルールのマッチングを検査する必要があります。これらの要件を満たすには、どのような対策を講じる必要がありますか？
A. デフォルトの IPS ポリシーを無効にし、グローバル ログを有効にします。
B. IPS ポリシーを構成し、グローバル ログを有効にします。
C. デフォルトの IPS ポリシーを無効にし、ルールごとのログ記録を有効にします。
D. IPS ポリシーを設定し、ルールごとのログ記録を有効にします。
Answer: B (メーッセージを残す**)**

最新問題**: 426**
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. coredump packet-engine 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
Answer: B (メーッセージを残す**)**
セクション: 管理とトラブルシューティング
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/ b_Command_Reference_for_Firepower_Threat_Defense/ac_1.html

最新問題**: 427**
ネットワーク管理者は先月のファイル レポートを確認し、exe を除くすべてのファイル タイプが削除されたことに気付きました。
不明な処理が表示されます。この問題の原因は何ですか？
A. マルウェア ライセンスが Cisco FTD に適用されていません。
B. Cisco FMC はインターネットに接続できず、ファイルを分析できません。
C. アクセス ポリシーにファイル ポリシーが適用されていません。
D. Spero ファイル分析のみが有効になります。
Answer: C (メーッセージを残す**)**
ファイルポリシーは、Cisco Firepower Threat Defense（FTD）デバイスが様々なタイプのファイルに遭遇した際に実行するアクションを定義します。ファイルポリシーは、アクセス制御ポリシーの一部として適用されます。アクセス制御ポリシーにファイルポリシーが含まれていない場合、FTDデバイスは遭遇したファイルに対して何のアクションも実行せず、exeファイルを除くすべてのファイルタイプに対して 不明」という処理結果を返します。

参照：
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-c

最新問題: **428**
パケットをドロップできるインターフェース タイプはどれですか?
A. 受動態
B. インライン
C. ERSPAN
D. タップ
Answer: B (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html

最新問題: **429**
ネットワーク管理者は、アクティブ/パッシブHAのCisco FTDペアを設定する際に、フェイルオーバーに使用するリンクを選択できません。高可用性ペアを設定する前に、どの設定を変更する必要がありますか？
A. インターフェイス上の各 Cisco FTD に、同じサブネット内の IP アドレスを追加する必要があります。
B. 各 Cisco FTD のインターフェイスからインターフェイス名を削除する必要があります。
C. 名前 Failover は、各 Cisco FTD のインターフェイスで手動で設定する必要があります。
D. インターフェイスは、LACP Active/Active EtherChannel の一部として設定する必要があります。
Answer: A (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

最新問題: **430**
エンジニアは、Cisco Secure Firewall Threat Defenseにスタティックルートトラッキングを実装し、プライマリパスに障害が発生した場合にバックアップパスを使用してトラフィックを再ルーティングする必要があります。エンジニアは既にプライマリスタティックルートを定義しており、プライマリパスは既に監視されています。この要件を満たすために、エンジニアはどのようなアクションを実行する必要がありますか？
A. IP SLA ICMP エコー要求を確立します。
B. 静的ルートの追跡オブジェクトを設定する
C. 静的ルートに一意の追跡IDを割り当てる
D. 優先順位の高いセカンダリスタティックルートを設定します
Answer: D (メーッセージを残す**)**
プライマリルートに障害が発生した場合に使用するバックアップスタティックルートを作成します。このルートのメトリックは、プライマリルートよりも大きくする必要があります。例えば、プライマリルートのメトリックが1の場合、バックアップルートのメトリックは10になります。通常、バックアップルートには別のインターフェースを選択します。
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/fdm/fptd-fdm-config-guide-700/fptd- fdm- routing.html#:~:text=プライマリ ルートが失敗した場合に使用するバックアップ スタティック ルートを作成します。このルートにはプライマリ ルートよりも大きなメトリックが必要です。たとえば、プライマリ ルートが失敗した場合は、仮想ルートはバックアップルートになる可能性がある

最新問題: **431**
クラスターユニット環境でサイト間 VPN を設定する場合の欠点は何ですか?
A. 障害が発生したマスター ユニットが回復した場合にのみ、VPN 接続を再確立できます。
B. すべてのクラスタ ユニット間で同時に VPN 接続を維持するには、スマート ライセンスが必要です。
C. 新しいマスター ユニットが選出された場合、VPN 接続を再確立する必要があります。

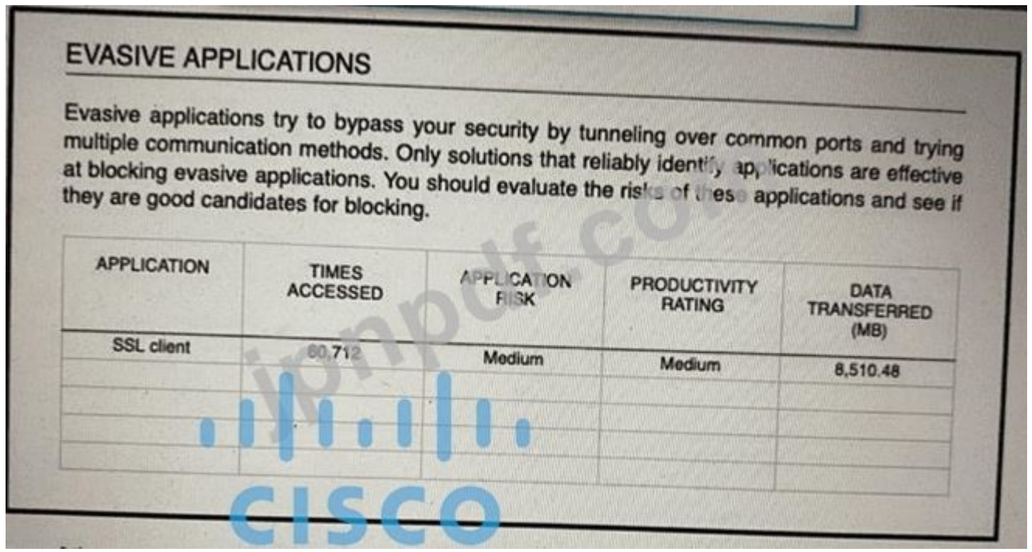
D. 新しいマスター ユニットが選出されると、確立された VPN 接続のみが維持されます。
Answer: (解答を表示する**)**
セクション: 構成
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster- solution.html#concept_g32_yml_y2b

最新問題**: 432**
Syslog を使用するのではなく、Cisco Firepower 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直接 Cisco Threat Response にイベントを送信する利点は何ですか?
A. Firepower 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。
B. すべてのタイプの Firepower デバイスがサポートされています。
C. サポートされているバージョンの Firepower を実行しているすべてのデバイスをサポートします。
D. オンプレミスのプロキシサーバーはセットアップやメンテナンスの必要がない
Answer: D (メーッセージを残す**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/ Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

最新問題**: 433**
ある企業は、4つのインターフェースペアを含む単一のインターフェースセットを持つインラインモード構成のCisco Secure IPSデバイスを導入しようとしています。IPSデバイスがパケットフローを一意に識別し、重複トラフィックや誤検知の報告を防ぐには、どの2つの設定を実装する必要がありますか？ 2つ選択してください。）
A. IPSインターフェースに接続されたスイッチの送信元SPANポートをtxのみに設定します。
B. Cisco Secure IPSデバイスで使用されるセキュリティゾーンを変更します
C. インラインセットのMTUを少なくとも1518に変更します
D. アクセスルールを再設定して、パケットの最初の出現以外をすべてドロップします。
E. インターフェースペアを別々のインラインセットに再割り当てします
Answer: B,E (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/ips_device_deployments_and_configuration.pdf

最新問題**: 434**
Threat Intelligence Director がサポートするフィルタリングの最大 SHA レベルは何ですか?
A. SHA-1024
B. SHA-4096
C. SHA-512
D. SHA-256
Answer: (解答を表示する**)**
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_directortid_.html

最新問題**: 435**
展示品を参照してください。



管理者がCisco Firepowerのレポート機能を確認していたところ、ネットワークリスクレポートのこのセクションに、回避に利用される可能性のあるSSLアクティビティが多数表示されていることに気づきました。このリスクを軽減するには、どのような対策を講じればよいでしょうか？

A. 暗号化されたトラフィック分析を使用して攻撃を検出する
B. Cisco Tetration を使用して、サーバへの SSL 接続を追跡します。
C. Cisco AMP for Endpoints を使用してすべての SSL 接続をブロックします
D. SSL 復号化を使用してパケットを分析します。

Answer: D (メーッセージを残す)

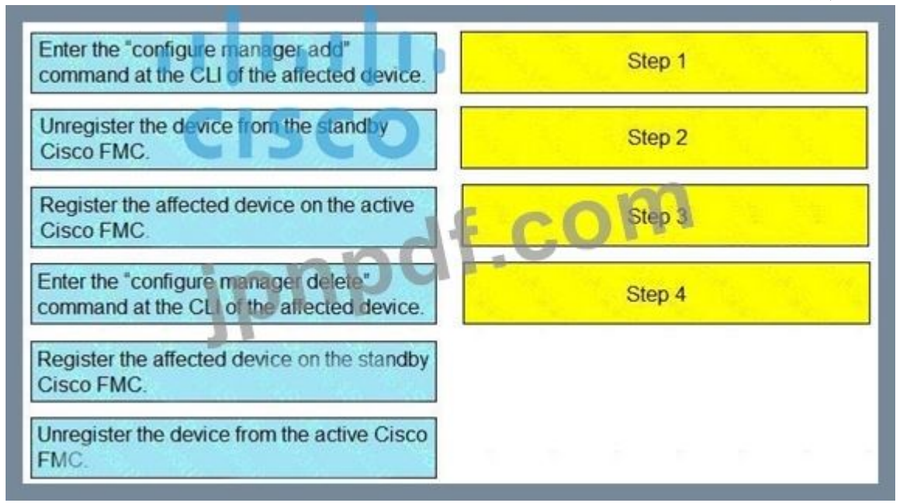
最新問題: **436**
高可用性をサポートする 2 つの展開タイプはどれですか (2 つ選択してください)。
A. シャーシ内マルチインスタンス
B. 透明
C. クラスター化された
D. ルーティング
E. パブリッククラウド内の仮想アプライアンス
Answer: (解答を表示する)

最新問題: **437**
セキュリティエンジニアは、ネットワークトラフィックの流れを中断することなく侵入イベントを検出するために、Cisco FTDアプライアンスをBump In The Wire（BIP）として導入する必要があります。このタスクを実行するには、どの2つの機能を設定する必要がありますか？（2つ選択してください。）

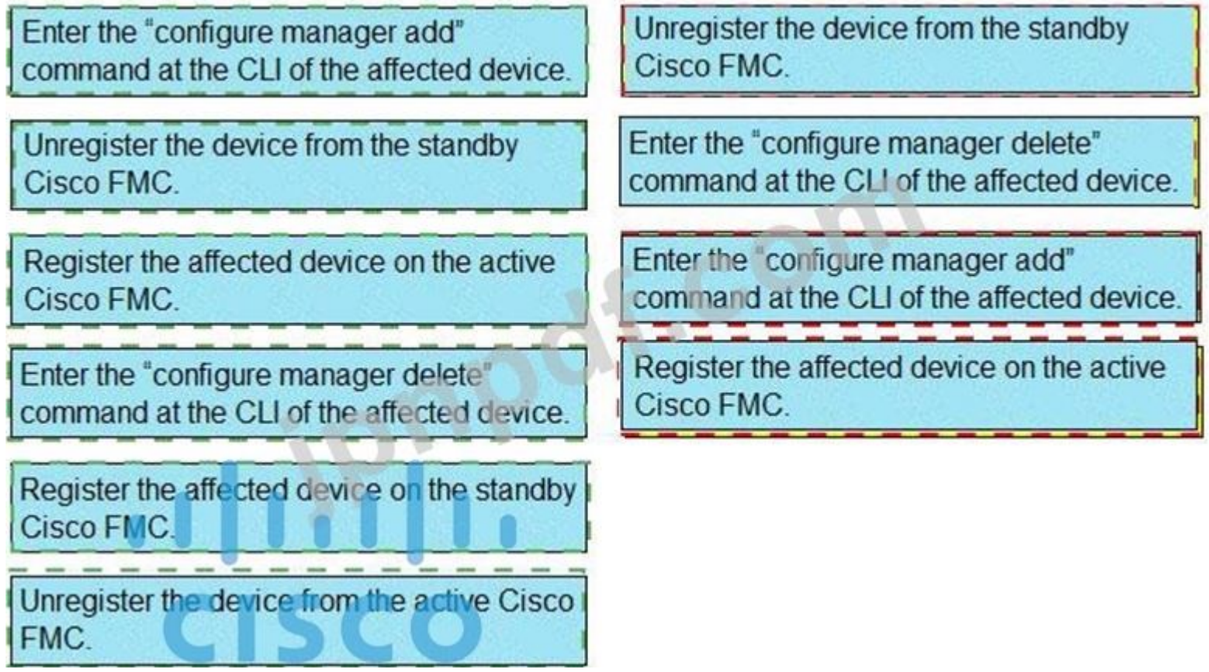
A. パッシブインターフェース
B. ブリッジモード
C. 透過モード
D. インラインセットペア
E. タップモード
Answer: D,E (メーッセージを残す)

最新問題: **438**
Cisco FTD 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. 冗長インターフェース
B. 動的ルーティングプロトコル
C. EtherChannelインターフェース
D. 高可用性クラスタ
Answer: A (メーッセージを残す)
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html#id_40010

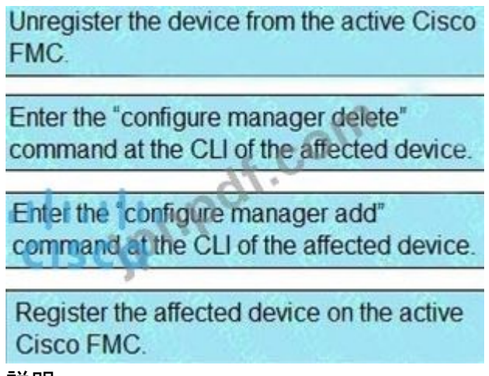
最新問題: **439**
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。



Answer:



説明



説明

参考 :https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

最新問題**: 440**

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

A. 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。

B. インライン タップ モードでは完全なパケット キャプチャが実行されます。

C. インライン モードでは SSL 復号化は実行できません。

D. インライン モードでは悪意のあるトラフィックがドロップされる可能性があります。

Answer: D (メーッセージを残す**)**

セクション: 展開

最新問題**: 441**

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
Answer: C (メーッセージを残す**)**
サポートされているオブジェクト オーバーライドは次のとおりです。
ネットワーク
ポート
VLANタグ
URL
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

最新問題: **442**
Cisco Secure Firewall Management Center のリスク レポート機能の属性は何ですか?
A. 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
B. 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
C. マルチドメインシステム内のすべてのドメインを含む
D. マルチドメインシステムに現在のドメインを含める
Answer: D (メーッセージを残す**)**

最新問題: **443**
Cisco Secure Firewall Management Center 管理対象デバイスで 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. 両方のユーザーからの変更がポリシーにマージされます。
C. 最初のユーザーは、ポリシーの編集を選択したときに構成をロックします。
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。
Answer: A (メーッセージを残す**)**
2人のユーザーが同時にリモートアクセスVPNポリシーを編集することはできません。ただし、Webインターフェースでは同時編集を防止できません。同時編集が発生した場合、最後に保存された設定が保持されます。
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/vpn-remote-access.html

最新問題: **444**
あるエンジニアが、Cisco FMC内に新しいダッシュボードを作成し、他の多くのダッシュボードのウィジェットを単一のビューにまとめようとしています。目標は、脅威とセキュリティ関連のウィジェットと、Cisco Firepowerデバイスのヘルス情報を組み合わせることです。
この情報を提供するには、どの 2 つのウィジェットを構成する必要がありますか? (2 つ選択してください。)
A. 侵入イベント
B. 相関情報
C. アプライアンスのステータス
D. 現在のセッション
E. ネットワークコンプライアンス

Answer: (解答を表示する)
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/dashboards.html#ID-2206-00000283

最新問題: **445**
管理者はネットワークをより適切にセグメント化するためにインターフェースオブジェクトを作成しようとしていますが、オブジェクトにインターフェースを追加する際に問題が発生しています。この失敗の原因は何ですか？
A. インターフェースは複数のネットワークの NAT に使用されています。
B. 管理者は複数のタイプのインターフェースを追加しています。
C. 管理者は複数のゾーンにあるインターフェースを追加しています。
D. インターフェースは複数のインターフェース グループに属しています。
Answer: (解答を表示する)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusa
インターフェース オブジェクト内のすべてのインターフェースは、すべて同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェース オブジェクトを作成した後は、含まれるインターフェースのタイプを変更することはできません。

最新問題: **446**
エンジニアは、既存の透過的な Cisco FTD をルーティング モードに変更したいと考えています。
デバイスは2つのネットワークセグメント間のトラフィックを制御します。変更後、ホストがこれらの2つのセグメント間の通信を再確立できるようにするために必須のアクションはどれですか？
A. 既存の動的ルーティング プロトコル設定を削除します。
B. セグメント間のルーティングを行うために複数の BVI を設定します。
C. 各セグメントに重複しない IP サブネットを実装します。
D. 各ファイアウォール インターフェイスに一意の VLAN ID を割り当てます。
Answer: C (メーッセージを残す)

最新問題: **447**
レポート テンプレートを作成するときに、特定のサブネットのアクティビティのみを表示するように結果を制限するにはどうすればよいですか?
A. Firepower Management Center でカスタム検索を作成し、レポートの各セクションで選択します。
B. レポートの詳細設定で入力パラメータを追加し、タイプをネットワーク/IP に設定します。
C. 検索フィールドが CIDR 形式のネットワークとして定義されたレポートにテーブル ビュー セクションを追加します。
D. レポートの各セクションで、X 軸として IP アドレスを選択します。
Answer: (解答を表示する)
https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Reports.html#87267

最新問題: **448**
ネットワーク管理者がパケットキャプチャを確認しています。Cisco Secure Firewall Threat Defense 内部からのパケットキャプチャには、受信 TCP トラフィックが表示されています。しかし、Secure Firewall Threat Defense 外部からのパケットキャプチャには、送信 TCP トラフィックが表示されません。どの設定変更でこの問題を解決できますか？
A. パケットキャプチャには UDP トラフィックを含める必要があります。
B. 宛先へのルートを追加する必要があります。
C. 内部インターフェースには、より低いセキュリティ レベルを割り当てる必要があります。
D. 内部インターフェースには、より高いセキュリティ レベルを割り当てる必要があります。

Answer: B (メーッセージを残す)

最新問題: **449**
エンジニアがセキュリティゾーンまたはトンネルゾーンにファイルポリシー設定を展開するアクセス制御ルールを設定したところ、デバイスが再起動しました。再起動の理由は何ですか？
A. ルール内のソース トンネル ゾーンが、ソース ポリシー内のトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
B. アクセス制御ルール内の送信元または宛先のセキュリティ ゾーンは、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致します。
C. ルール内のソース トンネル ゾーンが、宛先ポリシー内のトンネル ルールに割り当てられているトンネル ゾーンと一致しません。
D. ソース トンネル ゾーン内のソースまたは宛先セキュリティ ゾーンが、ターゲット デバイスのインターフェイスに関連付けられているセキュリティ ゾーンと一致しません。
Answer: (解答を表示する)

最新問題: **450**
エンジニアがCisco Secure EndpointとCisco Secure Firewall Management Centerを高可用性モードで統合しようとしています。Secure Endpointで検出されたマルウェアイベントは、Secure Firewall Management Centerでも受信する必要があり、パブリッククラウドサービスも利用しています。高可用性ピアの両方で個別に選択する必要がある2つの設定はどれですか？ 2つ選択してください。）
A. セキュリティグループタグ
B. セキュアエンドポイントクラウド接続
C. スマートソフトウェアマネージャーサテライト
D. インターネット接続
E. シスコ サクセス ネットワーク
Answer: (解答を表示する)
Cisco Secure Endpoint との統合を有効にしてマルウェア イベントを受信するには、各 FMC ピアで Secure Endpoint Cloud Connection を設定する必要があります。
Cisco Secure Endpoint を含むクラウドベースのサービスと通信するには、両方の高可用性ピアでインターネット接続が必要です。各ピアは独自のクラウド接続を管理するため、個別に設定する必要があります。

最新問題: **451**
FlexConfig を使用せずに Firepower Threat Defense でサポートされる動的ルーティング プロトコルはどれですか (2 つ選択してください)。
A. EIGRP
B. OSPF
C. 静的ルーティング
D. IS-IS
E. BGP
Answer: (解答を表示する)
OSPFとBGPはどちらもFlexConfigなしでSmart CLIで設定できます
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

Table 1. Supported Routing Protocols

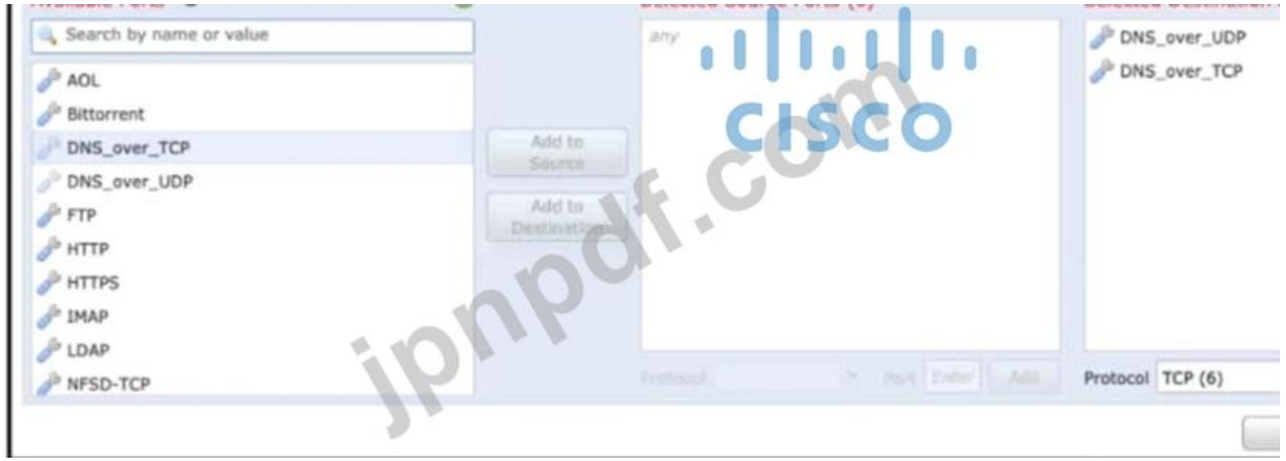
Routing Feature	Configuration Method	Notes
BGP	Smart CLI	Configure BGP Smart CLI objects from the **Device** > **Routing** page. Configure objects used in BGP, such as route maps, using Smart CLI objects from the **Device** > **Advanced Configuration** page.
Bi-directional forwarding detection (BFD)	FlexConfig	Configure BFD using FlexConfig objects from the **Device** > **Advanced Configuration** page. BFD is supported with BGP only.
EIGRP	FlexConfig	Configure EIGRP using FlexConfig objects from the **Device** > **Advanced Configuration** page.
IS-IS	FlexConfig	Configure IS-IS using FlexConfig objects from the **Device** > **Advanced Configuration** page.
Multicast routing	FlexConfig	Configure multicast routing using FlexConfig objects from the **Device** > **Advanced Configuration** page.
OSPFv2	Smart CLI	Configure OSPFv2 Smart CLI objects from the **Device** > **Routing** page. Configure objects used in OSPFv2, such as route maps, using Smart CLI objects from the **Device** > **Advanced Configuration** page.
OSPFv3	–	OSPFv3 configuration is not supported.
Policy-based routing (PBR)	FlexConfig	Configure policy-based routing (PBR) using FlexConfig objects from the **Device** > **Advanced Configuration** page.
RIP	FlexConfig	Configure RIP using FlexConfig objects from the **Device** > **Advanced Configuration** page.
Static routes	FDM	Configure static routes globally or per virtual router from the **Device** > **Routing** page.
Virtual routers, VRF	FDM	Configure virtual routers from the **Device** > **Routing** page.

最新問題**: 452**
エンジニアは、サービス グループ タグを使用している Cisco Firepower の接続の問題を調査しています。
特定のデバイスが正しくタグ付けされていないため、クライアントがファイアウォールを通過するときに適切なポリシーを使用できません。この問題はどのように解決されますか?
A. 一致基準を使用してパケット キャプチャを使用します。
B. 高度なオプションを指定した traceroute を使用します。
C. IP サブネット フィルターを使用して Wireshark を使用します。
D. 適切なフィルタリング機能を備えたパケットスニファーを使用する

Answer: (解答を表示する)

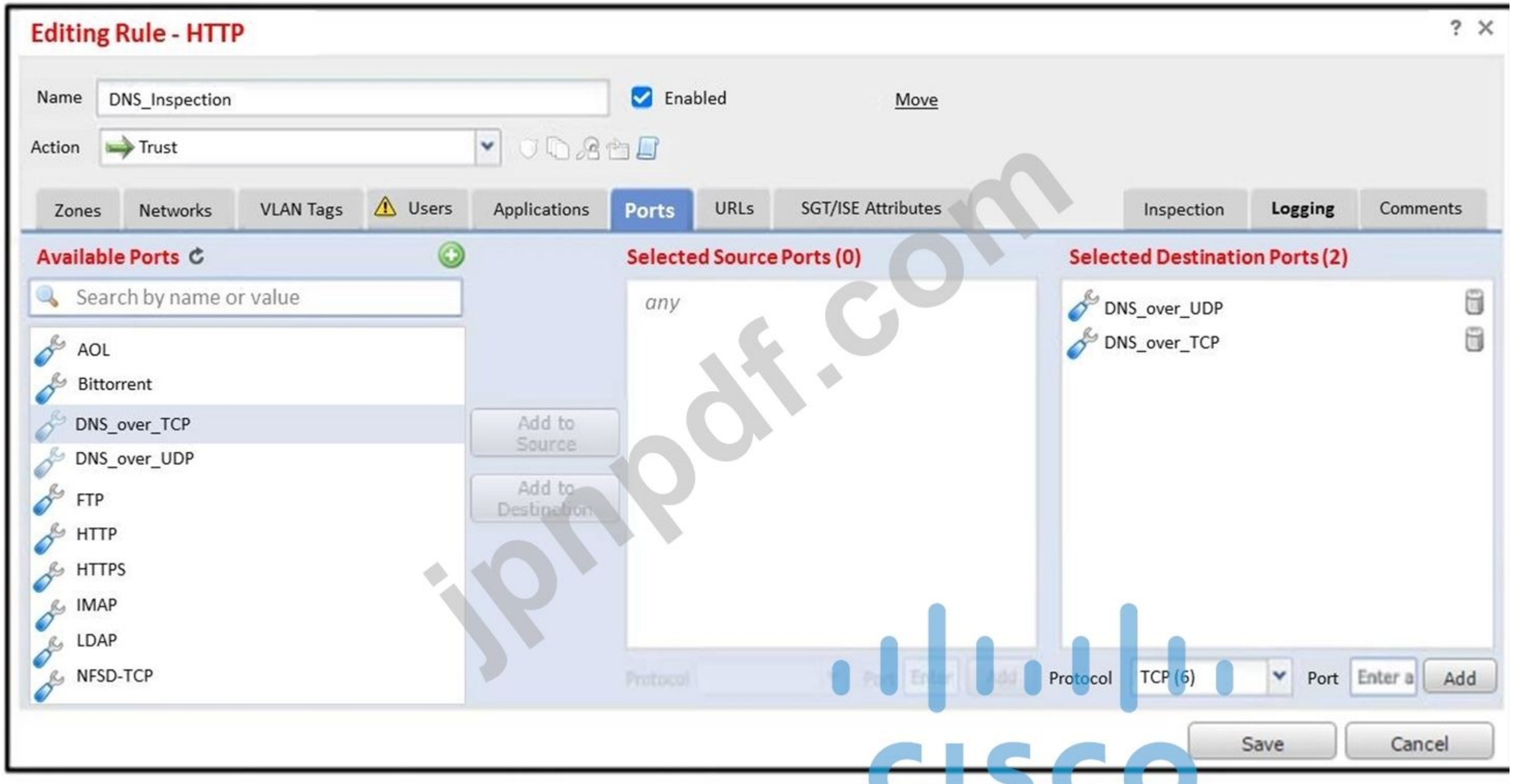
最新問題: **453**
ネットワーク管理者は、デバイスのすべての非管理インターフェースで検査が中断されていることに気づきました。原因は何でしょうか？
A. 管理以外のインターフェースに割り当てられた最高 MTU の値が変更されました。
B. 管理以外のインターフェースに割り当てられた最高 MSS の値が変更されました。
C. パッシブ インターフェイスがセキュリティ ゾーンに関連付けられました。
D. 同じインライン インターフェイスに複数のインライン インターフェイス ペアが追加されました。
Answer: (解答を表示する)
デバイス上のすべての非管理インターフェースの中で最大のMTU値を変更すると、設定変更の展開時にSnortプロセスが再起動され、トラフィックの検査が一時的に中断されます。検査は、変更したインターフェースだけでなく、すべての非管理インターフェースで中断されます。この中断によってトラフィックがドロップされるか、それ以上の検査を行わずに通過するかは、管理対象デバイスのモデルとインターフェースのタイプによって異なります。詳細については、「Snortの再起動によるトラフィックの動作」を参照してください。
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01101010.html

最新問題: **454**
展示品を参照してください。



エンジニアがアクセス制御ポリシーを変更し、通過するすべてのDNSトラフィックを検査するルールを追加しようとしたところ、変更を加えてポリシーを展開したところ、DNSトラフィックがSnortエンジンによって検査されていないことがわかりました。一体何が起こっているのでしょうか……
A. ルールの送信元ポートの設定が間違っています。
B. ルールでは、トラフィックの発信元となるセキュリティ ゾーンを指定する必要があります。
C. ルールでは、検査の送信元ネットワークとポートを定義する必要があります。
Answer: (解答を表示する)

最新問題: **455**
図を参照してください。エンジニアがアクセス制御ポリシーを変更し、ファイアウォールを通過するすべてのDNSトラフィックを検査するルールを追加しようとしています。変更を加えてポリシーを展開したところ、SnortエンジンによってDNSトラフィックが検査されていないことがわかりました。何が問題なのでしょうか？



A. ルールのアクションは、許可ではなく信頼に設定されています。
B. ルールでは、検査の送信元ネットワークとポートを定義する必要があります。
C. ルールでは、トラフィックの発信元となるセキュリティ ゾーンを指定する必要があります。
D. ルールの送信元ポートの設定が間違っています。
Answer: A (メーッセージを残す**)**
最新問題**: 456**
エンジニアがCisco FMG上で、コマンド restore remote-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Cisco FTDの設定を復元

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付けないエラーが発生しました。何が問題なのでしょうか？
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は適用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Cisco FTD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
Answer: D (メーッセージを残す)

最新問題: **457**
展示品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ましたが、サーバーからの応答がありません。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保証するには、どのアクションを実行すればよいですか？
A. ICMP トラフィックを許可するように Snort ルールを変更します。
B. ICMP 許可リストを作成し、ICMP 宛先を追加して暗黙的な拒否リストから削除します。
C. 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。
D. 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。
Answer: C (メーッセージを残す)

最新問題: **458**
ネットワーク管理者は、Cisco FTD 上の VPN ユーザー認証を LDAP から LDAPS に変換しようとしています。このタスクを完了するには、Cisco FTD オブジェクトに対してどのような操作を行う必要がありますか？
A. 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。
B. 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 Cisco FTD 接続要件を定義します。
C. 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。
D. 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。
Answer: A (メーッセージを残す)

最新問題: **459**
エンジニアは、NAT ID が ACME001、パスワードが Cisco388267669 である 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 ACME001 <登録キー> <FMC IP>
B. configure manager add <FMC IP> ACME0O1 <登録キー>
C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <登録キー>

D. configure manager add <FMC IP> 登録キー> ACME001
Answer: D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.html

最新問題**: 460**
FTD LINA エンジンはどの 2 つのパケット キャプチャをサポートしていますか? (2 つ選択してください。)
A. 動的ファイアウォールのインポート
B. レイヤー7ネットワークID
C. アプリケーションID
D. プロトコル
E. 送信元IP
Answer: D,E (メーッセージを残す**)**

最新問題**: 461**
エンジニアがCisco Secure Firewall Management Centerアプライアンスを導入しています。会社はCisco Secure Network Analyticsアプライアンスにデータを送信する必要があります。エンジニアが実行する必要がある2つのアクションはどれですか？ 2つ選択してください。）
A. NetFlow サービスを有効にするためにサービス識別子を作成します。
B. Netflow_Send_Destination オブジェクトを構成に追加します。
C. Netflow_Set_Parameters オブジェクトを構成に追加します。
D. Netflow_Add_Destination オブジェクトを構成に追加します。
E. Cisco Secure Network Analytics にデータを送信するためのセキュリティ インテリジェンス オブジェクト
Answer: C,D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure- netflow-secure-event-logging- o.html#:~:text=The%20four%20predefined%20objects%20are%20listed%20in%20the%20table%
3A

最新問題**: 462**
展示品を参照してください。

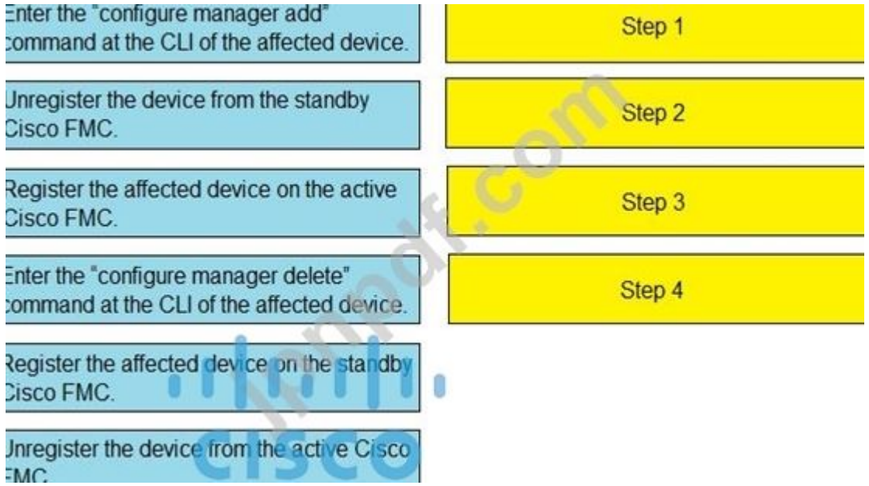
既存の Cisco FMC 構成の効果は何ですか?
A. 管理対象デバイスが Cisco FMC から削除されます。
B. Cisco FMC と管理対象デバイス間の通信用のリモート管理ポートがポート 8443 に変更されます。
C. Cisco FMC と管理対象デバイス間の SSL 暗号化通信チャネルがプレーンテキスト通信チャネルになります。

D. Cisco FMC と Cisco FTD 間の管理接続が無効になっています。
Answer: D (メーッセージを残す)

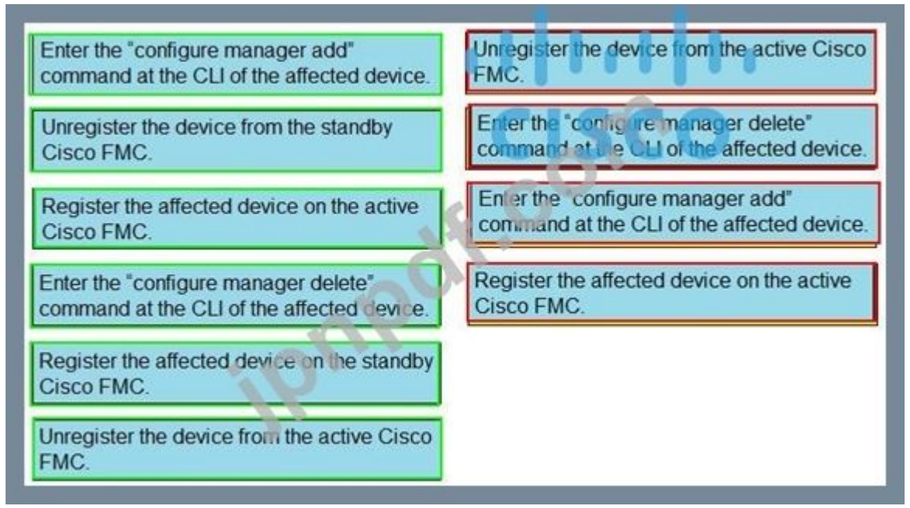
最新問題: **463**
エンジニアは、Cisco Secure Firewall Management Center を使用して生成されたリスクレポートを分析しています。レポートには以下のフィールドが含まれています。
- 総攻撃数
- 注意が必要なイベント
- ターゲットホスト
- CnCサーバーに接続されたホスト
エンジニアはどのような種類のリスクレポートを分析しているのでしょうか？
A. 攻撃
B. ネットワーク
C. イベント
D. ホスト
Answer: D (メーッセージを残す)
「標的ホスト」や「CnCサーバーに接続しているホスト」といったフィールドが存在することから、これはホストリスクレポートであることがわかります。このレポートはホストレベルのセキュリティ状況に焦点を当てており、脅威インテリジェンスとトラフィック分析に基づいて、どの内部システムが攻撃を受けているか、侵害を受けているか、または不審な動作をしているかを示します。

最新問題: **464**
2 つの Cisco FTD デバイス間で高可用性を実現するには、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設定
C. 同じDHCP/PPoE設定
D. 同じホスト名
E. インターフェースの数が同じ
Answer: (解答を表示する)
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html 条件 2 つの FTD デバイス間に HA を作成するには、次の条件を満たす必要があります。
同じモデル
同じバージョン（これは FXOS と FTD に適用されます - メジャー（最初の番号）、マイナー（2 番目の番号）、メンテナンス（3 番目の番号）は同じである必要があります）） 同数のインターフェイス、同じタイプのインターフェイス、両方のデバイスが FMC 内の同じグループ/ドメインの一部である、同一のネットワーク タイム プロトコル（NTP）設定がある、コミットされていない変更なしで FMC に完全に展開されている、同じファイアウォール モード（ルーテッドまたはトランスペアレント）である。
FTD が同じモードであっても、FMC がこれを反映しないケースがあるため、FTD デバイスと FMC GUI の両方でこれを確認する必要があることに注意してください。
いずれのインターフェースにもDHCP/Point-to-Point Protocol over Ethernet（PPPoE）が設定されていません。両方のシャーシで異なるホスト名（完全修飾ドメイン名（FQDN）が設定されています。シャーシのホスト名を確認するには、FTD CLIにアクセスし、次のコマンドを実行します。

最新問題: **465**
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。



Answer:



最新問題: **466**

2 つの Cisco FTD デバイス間で高可用性を実現するには、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DHCP/PPoE設定

B. インターフェースの数が同じ

C. 同じフラッシュメモリサイズ

D. 同じNTP設定

E. 同じホスト名

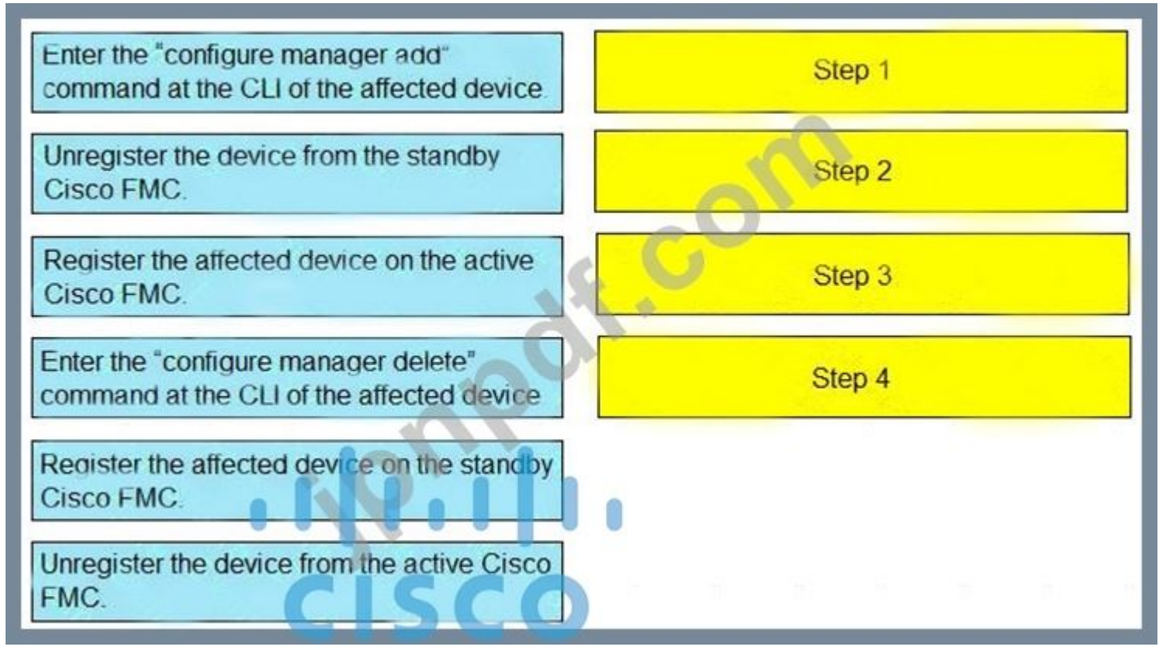
Answer: (解答を表示する**)**

最新問題: **467**
セキュリティエンジニアは、組織のSyslogサーバイベントを確認したところ、Cisco Secure Endpointを実行しているホストから悪意のあるサイトへのアウトバウンド接続が多数発生していることを確認しました。これらのホストは、Cisco FTDデバイスとは別のネットワーク上に存在します。これらの接続をブロックするには、どのようなアクションが必要ですか？
A. Cisco Secure Endpoint のポリシーを変更して、DFC を有効にします。
B. TetraおよびSperoエンジンを有効にしたCisco Secure Endpointポリシーを追加します。
C. 悪意のあるサイトのIPアドレスをCisco FMCのアクセス制御ポリシーに追加します。
D. Cisco FMCのアクセス制御ポリシーを変更して、悪意のあるアウトバウンド接続をブロックします。
Answer: C (メーッセージを残す**)**

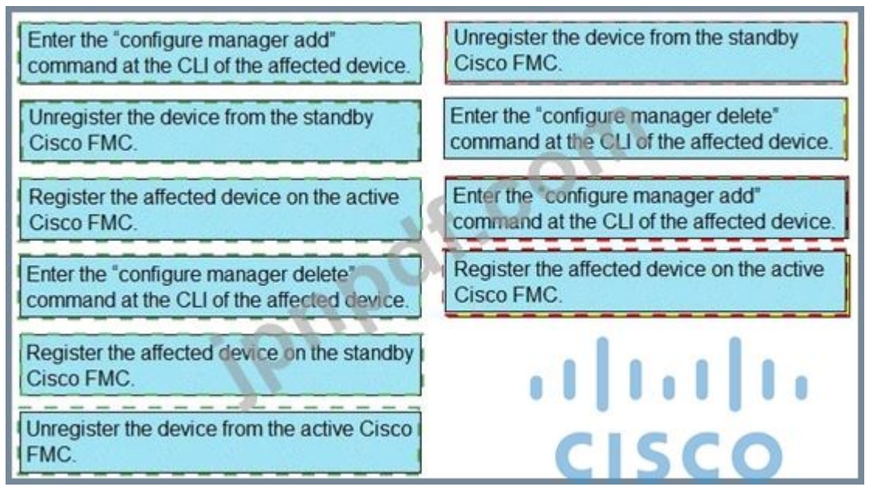
最新問題: **468**
エンジニアはCisco FTDデバイスを導入する必要があります。経営陣は、エンドユーザーに影響を与えるネットワーク変更を必要とせずにトラフィックを検査したいと考えています。企業のセキュリティポリシーでは、管理トラフィックとデータトラフィックを分離し、リモート管理にはTelnet経由のSSHを使用することが義務付けられています。これらの要件を満たすには、デバイスをどのように導入すればよいでしょうか？
A. 管理インターフェースを備えた透過モード
B. ブリッジ仮想インターフェースを使用したルーティングモード
C. データインターフェースで作成された透過的な
D. 診断インターフェースを備えたルーティングモード
Answer: A (メーッセージを残す**)**

最新問題: **469**
脅威対応チームは、脅威の分析と調査にシスコ社内のどのグループを使用していますか?
A. シスコ ディープ アナリティクス
B. OpenDNS グループ
C. シスコネットワークレスポンス
D. シスコ タロス
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

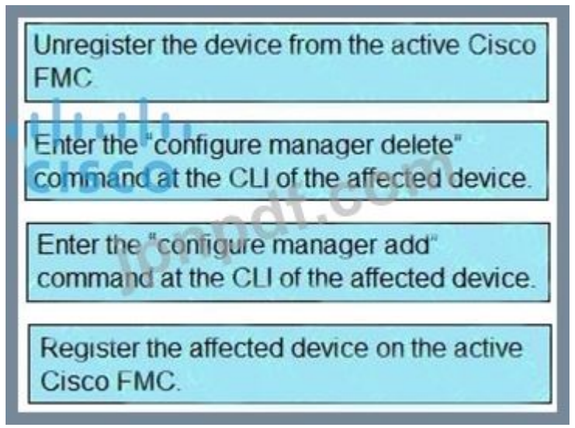
最新問題: **470**
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。


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

Answer:


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

説明



説明

参考 :https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

最新問題: **471**

ネットワーク管理者が攻撃リスクレポートを確認したところ、影響度が低い攻撃が複数あることに気づきました。このタイプの攻撃は何を示しているのでしょうか？

A. 手動で分類されるまで、すべての攻撃は低レベルとしてリストされます。

B. ホストはこれらの攻撃に対して脆弱ではありません。

C. 攻撃はネットワークにとって危険ではありません。

D. ホストは管理者の環境内にありません。

Answer: (解答を表示する)

説明

影響度の低い攻撃とは、ホストがそれらの攻撃に対して脆弱ではないことを意味します。影響度の低い攻撃とは、標的ホストの既知の脆弱性を悪用しない、またはFTDデバイス5のシグネチャや異常検出ルールに一致しない攻撃を指します。影響度の低い攻撃とは、攻撃がネットワークにとって危険ではない、あるいはホストが管理者の環境内に存在しないという意味ではありません。単に、攻撃によってホストが侵害されたり、影響を受けたりしなかったことを意味します。

その他のオプションは、次の理由により正しくありません。

すべての攻撃は、手動で分類されるまで 低」としてリストされるわけではありません。FTDデバイスは、脆弱性情報、脅威スコア、信頼度評価5など、さまざまな要素に基づいて、各攻撃に自動的に影響レベルを割り当てます。影響レベルは、攻撃の発生可能性と深刻度に応じて、高、中、低のいずれかになります。

攻撃は必ずしもネットワークに無害であるとは限りません。影響度の低い攻撃であっても、帯域幅の消費、ノイズの発生、他の攻撃からの注意の逸らしなど、ネットワークに何らかの損害や混乱を引き起こす可能性があります6。また、影響度の低い攻撃は、攻撃者がネットワークの潜在的な脆弱性や弱点を探査またはスキャンしていることを示唆している可能性もあります7。

ホストは必ずしも管理者の環境外にあるとは限りません。低影響度の攻撃は、場所や所有者に関わらず、ネットワーク上のあらゆるホストを標的とする可能性があります。低影響度の攻撃は、ホストが管理者の環境外にある、あるいは無関係であることを意味するものではありません。

最新問題: **472**

エンジニアは、Cisco FTD アプライアンスを IPS 専用モードで設定しており、Fail-to-Wire インターフェイスを利用する必要があります。

これらの要件を満たすにはどのインターフェース モードを使用する必要がありますか?

A. 受動態

B. ルーティング

C. 透明

D. インラインセット

Answer: D (メーッセージを残す)
セクション: 展開
説明/参考資料: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

最新問題: **473**
クラスターユニット環境でサイト間 VPN を設定する場合の欠点は何ですか?
A. 障害が発生したマスター ユニットが回復した場合にのみ、VPN 接続を再確立できます。
B. すべてのクラスタ ユニット間で同時に VPN 接続を維持するには、スマート ライセンスが必要です。
C. 新しいマスター ユニットが選出された場合、VPN 接続を再確立する必要があります。
D. 新しいマスター ユニットが選出されると、確立された VPN 接続のみが維持されます。
Answer: (解答を表示する)
参考: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_g32_yml_y2b

最新問題: **474**
スタンバイCisco FMCで自動デバイス登録の失敗を復元するための手順を、左側から右側の正しい順序にドラッグ＆ドロップしてください。すべてのオプションが使用されるわけではありません。

Answer: