

Cisco.300-710J.v2026-10-12.q207

試験コード：	300-710J
試験名称：	Securing Networks with Cisco Firepower (300-710日本語版)
認証ベンダー：	Cisco
無料問題の数：	207
バージョン：	v2026-10-12
ページの閲覧量：	102
問題集の閲覧量：	2177

<https://www.jpnsiken.com/shiken/Cisco.300-710J.v2026-10-12.q207.html>

質問: 1

セキュリティアナリストがネットワーク侵害の可能性を調査しています。アナリストは、Cisco Secure Firewall Management Center から不審なアクティビティに関するレポートを作成する必要があります。調査を支援するために、レポートに含めるべき詳細を 2 つ選択してください。

- A. ユーザーによるクライアントアプリケーション
- B. 侵入イベント
- C. ホスト接続
- D. 攻撃されたマシンの数
- E. ユーザー接続

正解: ([正解を表示します](#))

Intrusion events provide the detection evidence needed to understand which signatures fired, the affected source and destination addresses, event severity, protocol information, and other indicators associated with the suspected compromise. Host connections provide the corresponding network context, allowing the analyst to determine which systems communicated, when the sessions occurred, and which ports, applications, or protocols were involved. Together, these details connect security detections with the traffic flows that produced them and support reconstruction of the incident. Client applications by user and user connections are useful when the investigation is primarily identity-focused, but they do not provide the same direct combination of exploit evidence and host-level network activity. The number of attacked machines is an aggregate measurement and lacks the granular information necessary to investigate the suspicious communications and determine their cause.

質問: 2

エンジニアがLANスイッチで作業していて、Cisco IPSへのネットワーク接続がダウンしていることに気づきました。トラブルシューティングの結果、スイッチが期待どおりに機能していると判断されました。この障害が発生するために何を実装する必要がありますか。

- A. CiscoIPSはフェールオープンモードになるように設定されています
- B. リンクステート伝播が有効になっている
- C. CiscoIPSが検出モードで設定されている
- D. アップストリームルーターのルーティングプロトコルが正しく構成されていません

正解: ([正解を表示します](#))

質問: 3



図を参照してください。エンジニアが、以下のハードウェアデバイスとソフトウェアバージョンを備えた高可用性ソリューションを構成しています。FXOS SW 2.0(1.23) ソフトウェアを搭載した Cisco Secure Firewall 9300 セキュリティ アプライアンス 2 台、両方のアプライアンスに Cisco Secure Firewall Threat Defense 6.0.1.1 (ビルド 1023) がインストールされています。また、SW 6.0.1.1 (ビルド 1023) を搭載した Cisco Secure Firewall Management Center が 1 台あります。高可用性構成を完了するには、どの条件を満たす必要がありますか？

- A. 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。
- B. バージョン番号は同じパッチ番号である必要があります。
- C. 両方のファイアウォールは同じ数のインターフェースを持つ必要があります。
- D. DHCPは少なくとも1つのファイアウォールインターフェースで設定する必要があります。

正解: [\(正解を表示します\)](#)

質問: 4

エンジニアは、サードパーティのセキュリティ インテリジェンス テディを Cisco Secure Firewall Management Center に統合する必要があります。Secure Firewall Management Center はバージョン 6.2 3 で、メモリは 8 GB です。Throat Intelligence Director を実装するには、どの 2 つのアクションを実行する必要がありますか? (2つ選択してください。)

- A. バージョン 6.6 にアップグレードします。
- B. REST API アクセスを有効にします。
- C. TAXII サーバーの URL を追加します。
- D. 7 GB のメモリを追加します。
- E. TAXII サーバーを追加します。

正解: **A,C** ([コメントを发表する](#))

To integrate a third-party security intelligence feed with Cisco Secure Firewall Management Center (FMC) using Threat Intelligence Director (TID), the following actions are necessary:

Upgrade to version 6.6:The FMC must be running at least version 6.6 to support Threat Intelligence Director.

Version 6.2.3 does not support the necessary features for this integration.

Add the URL of the TAXII server:Threat Intelligence Director uses TAXII (Trusted Automated eXchange of Indicator Information) to pull threat intelligence data from third-party sources. The URL of the TAXII server must be added to the TID configuration in FMC.

Steps:

Upgrade FMC to version 6.6 or later.

In FMC, navigate toIntegration > Threat Intelligence Director.

Add a new TAXII server by entering the URL of the TAXII server.

These actions enable the integration of third-party threat intelligence feeds, enhancing the security capabilities of the FMC.

References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Threat Intelligence Director.

質問: 5

エンジニアは、Cisco FTD 上でパケットキャプチャを実行して、ホストが IP アドレスを使用していることを確認したいと考えている。

192.168.100.100 の MAC アドレスは 0042.7734.103 です。接続の問題のトラブルシューティングに役立ちます。パケットキャプチャ出力に MAC アドレスが表示されるようにするための正しい tcpdump コマンド構文は何ですか？

A. -nm src 192.168.100.100

B. -s 1518 host 192.168.100.100

C. -w capture.pcap -s 1518 host 192.168.100.100 mac

D. -w capture.pcap -s 1518 host 192.168.100.100 ether

正解: ([正解を表示します](#))

Reference:<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

質問: 6

Cisco FMC 管理者は、信頼できるネットワークトラフィックの高速パスを設定して、パフォーマンスを向上させたいと考えています。管理者はどのタイプのポリシーでこの機能を構成しますか？

A. アイデンティティポリシー

B. 侵入ポリシー

C. ネットワーク分析ポリシー

D. プレフィルタポリシー

正解: ([正解を表示します](#))

質問: 7

コンサルタントは、顧客がFDMで管理されている単一の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取り組んでいます。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、その後、高可用性ペアを作成するために追加されるデバイスに複製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アクションを実行す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 に手動で構成する必要があります。

B. デバイスが登録されると、現在の FDM 構成は自動的に FMC に変換されます。

C. 現在のFDM構成は、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 の設定を ASA コマンド形式に変換し、その後 FMC に移行する必要があります。

正解: ([正解を表示します](#))

When an FTD device that is managed by FDM is registered to FMC, the existing configuration is automatically converted and imported into FMC. The FMC then pushes the configuration back to the device.

This process preserves most of the FDM configuration, except for some features that are not supported by FMC, such as VPN wizards and certificates.

質問: 8



図を参照してください。ユーザーは、さまざまなTCPポートを使用して多数の外部リソースに接続しようとしています。ユーザーがポート番号を間違えると、接続は即座に切断され、接続が完全に切断されるまでに1分以上かかります。エンジニアは、図に示すように、両方のタイプの接続をキャプチャすることに成功しました。

エンジニアは、2番目の接続グループのタイムアウト値を下げてユーザーの問題を解決するために、どのような設定を行う必要があるでしょうか？

- A. ICMPプロトコルスイート全体を許可する送信アクセスルール
- B. 外部からのTCPリセットパケットを許可する受信アクセスルール
- C. リセットアクション付きブロックの送信アクセスルール

正解: ([正解を表示します](#))

質問: 9

Cisco Firepower Threat Defenseソフトウェアでは、アプライアンスを通過するトラフィックを受動的に受信するように構成する必要があるインターフェイスモードはどれですか。

- A. インラインセッ
- B. パッシブ
- C. ルーティング済み
- D. インラインタッ

正解: ([正解を表示します](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/interface_overview_for_firepower_threat_defense.html

質問: 10

エンジニアがCiscoFTDアプライアンスをIPS専用モードで設定しており、フェイルトウワイヤ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、どのインターフェイ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. パッシブ
- D. インラインセット

正解: ([正解を表示します](#))

Reference: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

質問: 11

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

- A. SSL
- B. SSH
- C. IPsec
- D. MACsec

正解: C ([コメントを發表する](#))

質問: 12



図を参照してください。エンジニアがアクセス制御ポキーを変更して、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。変更を行い、ポキーを展開した後、DNS トラフィックが Snort エンジンによって検査されていないことがわかりました。問題は何ですか？

- A. ルールは、検査対象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が、許可ではなく信頼に設定されています。
- D. ルールは、送信元ポートの設定が間違っています

正解: ([正解を表示します](#))

質問: 13

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

Apps Associated with High Impact Events	Count	Apps Associated with Low Impact Events	Count
DNS	16	Chrome	283
Internet Explorer	14	Internet Explorer	110
Web browser	8	DCE/RPC client	74
FTP client	6	Web browser Firefox	47
NetBIOS-ssn (SMB) client	6	Firefox	36

OP ATTACKERS AND TARGETS

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

High Impact Events

Attackers	Attacks	Targets	Attacks
5.196.214.27	3	31.31.196.236	6
10.1.115.12	3	185.118.166.155	6
10.1.115.12	3	37.48.82.212	4
10.1.26.6	2	185.86.77.12	4
10.1.39.21	2	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向上させる必要があります、経営陣の承認を得るためにリスク軽減戦略を作成してい
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行動をとるべきでしょうか？

- A. TCPポート80のトラフィックを検査します。
- B. DNSトラフィックを検査します。
- C. Internet Explorerをブロックします。
- D. NetBIOSをブロックします。

正解: (正解を表示します)

質問: 14

組織は、ネットワークでトランスペアレント モードを使用して Cisco FTD を実装しています。デフォルトのアクセス コントロール ポリシーで、この展開
がネットワーク内にループを作成しないことを保証するルールはどれですか？

- A. STP BPDU パケットはデフォルトで許可されます。

- B. ARP パケットはデフォルトで許可されます。
- C. ARP インスペクションはデフォルトで有効になっています。
- D. マルチキャストおよびブロードキャスト パケットはデフォルトで拒否されます。

正解: **D** ([コメントを发表する](#))

質問: 15

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づきました。エンジニアは、この問題を解決するためにどの操作を行う必要がありますか？

- A. パケット 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. バッファ サイズを指定します。
- D. トレース オプションを有効にします。

正解: ([正解を表示します](#))

質問: 16

pxGrid Adaptive Network ControlをCisco ISEおよびCisco Secure Firewall Management Centerと統合することで、Cisco Rapid Threat Containmentのどの緩和策が有効になりますか？

- A. ブロック
- B. 拒否
- C. 終了
- D. 一時停止

正解: **A** ([コメントを发表する](#))

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

GigabitEthernet0/0	outside	Physical	outside_zone	209.165.201.2/30(Static)	Global
GigabitEthernet0/1	inside	Physical	inside_zone	192.168.1.1/24(Static)	Global
GigabitEthernet0/2	public	Physical	public_zone	209.165.201.5/30(Static)	Global

Name	Value	Type
obj_192.168.1.0_24	192.168.1.0/24	Network
obj_192.168.1.1_32	192.168.1.1	Host
obj_192.168.1.254_32	192.168.1.254	Host
obj_192.168.2.0_24	192.168.2.0/24	Network
obj_209.165.201.1_32	209.165.201.1	Host
obj_any	0.0.0.0/0	Network

Network	Interface	Leaked from Virtual Router	Gateway
obj_192.168.2.0_24	inside	Global	obj_192.168.1.254_32
any-ipv4	outside	Global	obj_209.165.201.1_32

図を参照してください。エンジニアは、クライアントが直接接続された内部ネットワークにある場合にのみインターネットを使用できるようにする NAT ルールを設定します。動的自動 PAT を設定する必要があります。左側の NAT ルールを右側の対応するターゲットにドラッグアンドドロップします。すべてのオプションが使用されるわけではありません。

auto NAT

outside_zone

obj_192.168.2.0_24

obj_192.168.1.0_24

inside_zone

dynamic

destination interface IP

NAT rule

type

source interface objects

destination interface objects

original source

translated source

正解:

auto NAT

outside_zone

obj_192.168.2.0_24

obj_192.168.1.0_24

inside_zone

dynamic

destination interface IP

auto NAT

dynamic

inside_zone

outside_zone

obj_192.168.1.0_24

obj_192.168.2.0_24

Explanation:

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



質問: 18

ユーザーは、Cisco Secure Firewall Threat Defense (FTD) デバイスで VPN に接続しようとする Cisco Duo 2FA が失敗すると報告しています。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。Cisco Secure Firewall Management Center (FMC) で VPN トラブルシューティング ログを表示すると、ネットワーク管理者は Cisco Duo AAA サーバーが failed としてマークされているというエラーを確認します。この問題の根本原因は何ですか？

- A. セキュア FMC 管理デバイスでは、多要素認証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 信頼証明書がありません。

正解: ([正解を表示します](#))

If users report that Cisco Duo 2FA fails when attempting to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device, and the VPN troubleshooting log in FMC shows an error indicating that the Cisco Duo AAA server has been marked as failed, the root cause is likely missing Duo trust certificates on the FTD device. Trust certificates are essential for establishing a secure and trusted connection between the FTD and the Duo authentication service.

Steps:

Obtain the necessary Duo trust certificates.

Install the certificates on the FTD device.

Verify the configuration to ensure that the FTD device can properly communicate with the Duo AAA server.

This resolves the authentication failure by ensuring that the FTD device can trust the Duo server.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Certificate Management.

質問: 19

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 Cisco Threat Response にイベントを直接送信することの利点は何ですか？

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

正解: ([正解を表示します](#))

質問: 20

エンジニアは、アクセス コントロール ポリシーの設定中に新しいルールを定義します。ポリシーを導入した後、ルールが期待どおりに機能せず、ルールに関連付けられているヒット カウンタがゼロを示しています。このエラーの原因は何ですか？

- A. ルールは作成後に有効化されませんでした。
- B. Snort の間違ったソース インターフェイスがルールで選択されました。
- C. ルールに対してロギングが有効になっていません。
- D. ルールで誤ったアプリケーション署名が使用されました。

正解: ([正解を表示します](#))

質問: 21

感染したエンドポイントが特定された場合の RTC ワークフローとは何ですか？

- A. Cisco ISE は、感染したエンドポイントを封じ込めるように Cisco FMC に指示します。
- B. Cisco ISE は、感染したエンドポイントを封じ込めるように Cisco AMP に指示します。
- C. Cisco FMC は、感染したエンドポイントを封じ込めるように Cisco ISE に指示します。
- D. Cisco AMP は、感染したエンドポイントを封じ込めるように Cisco FMC に指示します。

正解: C ([コメントを發表する](#))

質問: 22

エンジニアは、Secure Firewall Threat Defense デバイスの問題のトラブルシューティングを支援するために、Cisco Secure Firewall Management Center からパケットキャプチャをエクスポートする必要があります。エンジニアが Secure Firewall Management Center の URL にアクセスすると、次のようになります。

.. < FMC IP > /capture/CAP/pcap/sample.pcap

エンジニアは、PCAP ファイルを受け取る代わりに、403: Forbidden エラーを受け取りました。この問題を解決するには、どのような対処法が有効でしょうか？

- A. HTTPS サーバーを無効にして HTTP を使用します。
- B. デバイスプラットフォームポリシーでプロキシ設定を有効にします。
- C. デバイスプラットフォームポリシーで HTTPS を有効にします。
- D. クライアントブラウザのプロキシ設定を無効にします。

正解: ([正解を表示します](#))

If an engineer receives a 403: Forbidden error when attempting to download a packet capture file from Cisco Secure Firewall Management Center (FMC), the issue is likely due to HTTPS not being enabled in the device platform policy. To resolve this issue, the engineer must enable HTTPS in the platform policy.

Steps:

In FMC, navigate to Policies > Device Management > Platform Settings.

Edit the relevant platform policy.

Enable HTTPS for the device.

Deploy the changes to the FTD device.

This ensures that the FMC and FTD device can securely transfer the packet capture file over HTTPS, resolving the 403 error.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings and HTTPS Configuration.

質問: 23

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 データベースに現在登録されているルールのうち、まだ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、必要以上のルールは有効にたくありません。これらの要件を満たすアクションはどれですか？

- A. 使用中のポリシー内のルール状態を変更します。
- B. 基本ポリシーを「接続性よりもセキュリティ」に変更します。
- C. ポリシー内のルールの動的状態を変更します。
- D. 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。

正解: ([正解を表示します](#))

質問: 24

Cisco FMCの迅速な脅威封じ込めで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. pxGrid
- B. SGT
- C. BFD
- D. SNMP v3

正解: A ([コメントを发表する](#))

質問: 25

ネットワークエンジニアは、別のIPサブネットを作成せずに、トラフィック検査のためにFTDデバイスを介してユーザーセグメントを拡張しています。これは、ルーティングモードのFTDデバイスでどのように実現されますか？

- A. ARPを活用してトラフィックをファイアウォール経由で転送する
- B. インラインセットインターフェイスを割り当てる
- C. BVIを使用して、ユーザーセグメントと同じサブネットにBVIIPアドレスを作成します
- D. プレフィルタールールを活用してプロトコル検査をバイパスする

正解: C ([コメントを发表する](#))

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

質問: 26

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

A. Windowsドメインコントローラ

B. 監査

トリアージ

C. 保護

正解: **B** ([コメントを发表する](#))

Reference: <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html>

質問: 27

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

A. デバイス、リモート アクセス VPN

B. システム、レルム

C. ポリシー、認証

D. 認証、デバイス

正解: **B** ([コメントを发表する](#))

To configure Active Directory authentication for VPN authentication on a Cisco Secure Firewall Threat Defense (FTD) instance registered with Cisco Secure Firewall Management Center (FMC), the administrator needs to configure Realms in the System settings of the FMC. Realms in FMC are used to define the directory servers (e.g., Active Directory) and how they are used for user authentication.

Steps to configure this in FMC:

Navigate to System > Integration > Realms and Directory.

Add a new realm and configure the necessary details such as the directory server type (e.g., Active Directory), server address, and bind credentials.

Test the connection to ensure it works correctly.

This setup allows the FMC to authenticate VPN users against the Active Directory, thereby enabling secure access control for VPN connections.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Realms Configuration.

質問: 28

ある組織は、HTTPトラフィックをブロックする際に、Cisco Firepowerのデフォルトのブロックページを使用しないことを望んでいます。

組織は、ブロックが発生した際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含めたいと考えています。これらの要件を満たすために、どの2つの手順を実行する必要がありますか？(2つ選択してください。)

A. ポリシーと手順に関する情報を含むCSSコードを記述します。

B. アクセス制御ポリシーの HTTP リクエスト処理を編集して、カスタムブロックします。

C. アクセス制御ポリシーの HTTP レスポンスをカスタムに変更します。

D. Pythonを使用して、システムが提供するブロックページの結果を変更します。

E. ポリシーと手順に関する情報を含むHTMLコードを作成します。

正解: ([正解を表示します](#))

質問: 29

エンジニアは、現在の6.2.3展開にCisco FTDバージョン6.2.3デバイスを追加して、ハイアベイラビリティペアを作成したいと考えています。現在展開されているCiscoFTDデバイスは、ローカル管理と、使用可能なポート密度を含む同一のハードウェアを使用して、適切なハイアベイラビリティ展開に必要なフェールオーバーとステートフルリンクを有効にします。環境が新しいCiscoFTDを古いものとペアリングする準備ができていることを確認するアクションはどれですか。

- A. フェールオーバーインターフェイス用に、2つのデバイスに169.254.0.0/16の範囲のIPアドレスが割り当てられていることを確認します。
- B. 名前解決のために、構成されたDNSサーバーが2つのデバイスで一致していることを確認します。
- C. 両方のデバイスでCiscoFDM管理からCiscoFMC管理に変更し、FMCに登録します。
- D. 現在のCisco FTDを工場出荷時の状態にリセットして、設定を新しいCiscoFTDデバイスと同期できるようにします。

正解: [\(正解を表示します\)](#)

質問: 30

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ますが、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際に、システムが情報を表示するために必須となるオプションはどれですか？

- A. 表
- B. フィルター
- C. タイトル
- D. 結果

正解: C ([コメントを發表する](#))

When configuring a custom widget on a dashboard within Cisco Secure Firewall Management Center (FMC), it is mandatory to provide a title for the system to display the information correctly. The title helps in identifying and organizing the widget on the dashboard.

Steps:

Navigate to the dashboard section in FMC.

Add a new custom widget.

Configure the widget settings and provide a title.

Save and apply the widget to the dashboard.

Providing a title ensures that the widget is correctly displayed and easily identifiable on the dashboard.

References: Cisco Secure Firewall Management Center User Guide, Chapter on Dashboard and Custom Widgets.

質問: 31

Cisco ASA Firepowerモジュールを導入する場合、組織はネットワークに影響を与えずにトラフィックの内容を評価したいと考えています。現在、物理アプライアンス上に同じデバイスの複数のインスタンスを持つように構成されています。組織のニーズを満たす展開モードはどれですか。

- A. インラインタップモニター専用モード
- B. パッシブモニター専用モード
- C. パッシブタップモニターのためのモード
- D. インラインモード

正解: A ([コメントを發表する](#))

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access-sfr.html>

Inline tap monitor-only mode (ASA inline)-In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **32**

Cisco Firepower Management Center内で、ユーザーはどこでウィジェットを追加または変更しますか？

- A. ダッシュボード
- B. レポート
- C. コンテキストエクスプローラー
- D. サマリーツール

正解: ([正解を表示します](#))

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

質問: **33**

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

図を参照してください。エンジニアは、CSVファイルを使用して3つのネットワークオブジェクトをCisco Secure Firewall Management Centerにインポートする必要があります。このタスクを実行するには、CSVファイルでどのヘッダーを設定する必要がありますか？

- A. 名前; 説明; タイプ; 値; DN;
- B. 名前;説明; タイプ;値;DN;
- C. 名前;説明;タイプ;値;検索;
- D. 名前; 説明; タイプ; 値; ルックアップ;

正解: ([正解を表示します](#))

質問: **34**

Cisco FMCがCisco ISEと統合されている場合、どの2つの修復オプションを使用できますか？ (2つ選択してください。)

- A. 構成された動的nullルート
- B. DHCPプールの無効化
- C. 検疫
- D. ポートのシャットダウン
- E. ホストのシャットダウン

正解: ([正解を表示します](#))

Reference: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediati.html>

質問: 35

ある組織では、ブリッジグループを使用して内部インターフェースから外部インターフェースへのトラフィックを通過させるCisco FTDを使用しています。しかし、隣接するCiscoデバイスに関する情報を収集したり、環境内でマルチキャストを使用したりすることができません。この問題を解決するにはどうすればよいでしょうか？

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

正解: [\(正解を表示します\)](#)

" In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule... " " The bridge group does not pass CDP packets packets... " <https://www.cisco.com/c/en/us/td/docs/security/asa>

</asa913/configuration/general/asa-913-general-config/intro-fw.html>

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):

IP traffic-In routed firewall mode, broadcast and " multicast traffic is blocked even if you allow it in an access rule, " including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).

Non-IP traffic-AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.

Note

" The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

質問: 36

管理者は、Cisco Secure Firewall Threat Defenseデバイスを透過モードで設定します。BVI (ブリッジ仮想インターフェイス)を設定するには、管理者は以下の手順を実行する必要があります。

ブリッジグループインターフェイスを追加する

ブリッジグループIDを設定する

ブリッジグループインターフェイスの説明を設定する

ブリッジグループメンバーインターフェイスを追加する

エンジニアはこれらのアクションをどのように実行する必要がありますか？

- A. ブリッジグループインターフェイスのセキュリティゾーンを設定する
- B. ブリッジグループインターフェイスの名前を設定します
- C. ブリッジグループインターフェイスのIPアドレスを設定する
- D. ブリッジグループインターフェイスモードを透過に設定する

正解: C ([コメントを发表する](#))

質問: 37

スイッチドFirepowerデバイスの展開でネットワークの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

正解: ([正解を表示します](#))

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

質問: 38

ネットワーク管理者は、パブリックIPアドレスを内部WebサーバーのIPアドレスに変換するNATポリシーを構成しました。どのソースもポート80のパブリックIPアドレスに到達できるようにするアクセスポリシーも作成されています。インターネットからポート80でWebサーバーにアクセスすることはできません。どの構成変更が必要ですか。

- A. 送信元IPアドレスと宛先IPアドレスを変換するには、NATポリシーを変更する必要があります。
- B. アクセスポリシールールは、アクションの信頼のために構成する必要があります。
- C. 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。
- D. ポート80では侵入ポリシーを無効にする必要があります。

正解: C ([コメントを發表する](#))

質問: 39

エンジニアが、ペアの Cisco Secure Firewall デバイスのフェイルオーバー機能を展開しています。コア スイッチは、以前アクティブだったユニットの MAC アドレスを ARP テーブルに保持します。Cisco Secure Firewall のフェイルオーバー後もネットワーク ユーザーがインターネットにアクセスできるように、ダウンタイムを最小限に抑えるには、エンジニアはどの操作を行う必要がありますか？

- A. 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。
- B. MAC アドレスをスイッチの ARP テーブルに追加します。
- C. 両方のユニットで同じ MAC アドレスを設定します。
- D. 両方のユニットで仮想 MAC アドレスを使用します。

正解: ([正解を表示します](#))

質問: 40

トラフィックが明示的に破棄されない限り、すべてのトラフィックを受信して再送信する必要があるIPSを実装する場合、Cisco Secure Firewall Threat Defenseのどのインターフェイスモードを導入する必要がありますか？

- A. ルーティング済み
- B. インライン
- C. 受動
- D. 透明

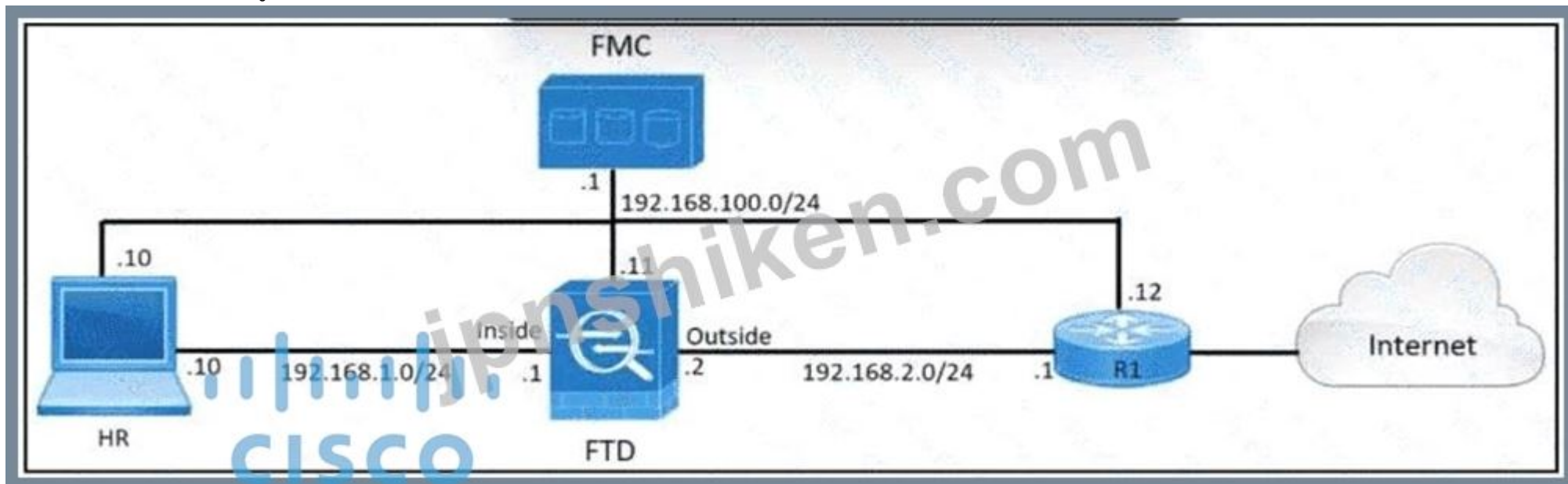
正解: ([正解を表示します](#))

An inline set consists of paired Secure Firewall Threat Defense interfaces placed directly in the network traffic path. The interfaces operate like a bump in the wire: one interface receives the traffic, the inspection engine evaluates it, and the paired interface retransmits it unless an access-control, intrusion, file, or other security policy explicitly drops it. This arrangement enables the IPS to prevent attacks because the device can stop malicious packets before

forwarding them. A passive interface also receives traffic unconditionally, but it receives copied traffic from a SPAN or mirror port and retransmits none of it. Routed and transparent modes describe broader firewall packet-forwarding behavior rather than this IPS-only interface characteristic. Therefore, an inline deployment satisfies the requirement to inspect, retransmit, and selectively drop traffic.
Cisco inline-set documentation

質問: 41

図を参照してください。



エンジニアは、人事部のユーザーから発信される HTTP および HTTPS トラフィックを制限するために、Cisco Secure Firewall 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 トラフィックのダウンロードとアップロードの制限は両方とも 5 Mb/s に設定する必要があります。対応する QoS ルール設定に値をドラッグアンドドロップします。

192.168.1.0/24	Name
192.168.2.0/24	
HTTP-HTTPS	Apply QoS On
HTTP-HTTPS-QoS	
5 Mb/s	Download/Upload Limit
Interfaces in Destination Interface Objects	
	Source Interface Networks
	Destination Interface Networks
	Destination Ports

正解:



Explanation:

Name # HTTP-HTTPS-QoS

Apply QoS On # Interfaces in Destination Interface Objects

Download/Upload Limit # 5 Mb/s

Source Interface Networks # 192.168.1.0/24

Destination Interface Networks # 192.168.2.0/24

Destination Ports # HTTP-HTTPS

The HR workstation resides on the inside 192.168.1.0/24 network, making that subnet the source-interface network. Internet-bound traffic exits through the 192.168.2.0/24 network, which must be configured as the destination-interface network. Because rate limiting must occur as traffic leaves toward the internet, QoS is applied to interfaces in the destination interface objects. The HTTP-HTTPS object identifies the destination ports for web traffic, while HTTP-HTTPS-QoS provides a descriptive rule name. Both download and upload limits are configured as 5 Mb/s. Cisco Secure Firewall applies a QoS limit

independently on each selected interface and determines upload and download direction based on the connection initiator. The Apply QoS On selection must correspond to a populated source or destination interface condition. Cisco Secure Firewall QoS configuration

質問: 42

Cisco FTDのブリッジグループの特徴は何ですか？

- A. ルーテッドファイアウォールモードでは、ブリッジグループ間のルーティングがサポートされています。
- B. ブリッジグループ間のルーティングは、接続されたルーターのルーターオンスティック構成でのみ実現されます。
- C. 透過ファイアウォールモードでは、ブリッジグループ間のルーティングがサポートされています
- D. ルーテッドファイアウォールモードでは、ブリッジグループ間のルーティングはルーテッドインターフェイスを通過する必要があります。

正解: A ([コメントを発表する](#))

質問: 43

ネットワーク管理者が毎週の攻撃リスクレポートを確認している際に、インパクトレベル2の攻撃が疑われる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 > 検索 > 全体
- B. 分析 > 関連 > 関連イベント
- C. 分析 > ホスト > 脆弱性
- D. 分析 > ホスト > ホスト属性

正解: C ([コメントを発表する](#))

The Analysis > Hosts > Vulnerabilities page in Cisco FMC displays information about the hosts on the network and their associated vulnerabilities. The administrator can filter the hosts by impact level, which indicates how likely an attack is to succeed against a host. An impact level of 2 means that the host was attacked and is potentially vulnerable, but no exploit was confirmed. The administrator can click on a host to view more details, such as its IP address, operating system, applications, protocols, and intrusion events. The administrator can also view the details of each vulnerability, such as its CVE ID, description, severity, and recommended actions³

質問: 44

Cisco FMC GUIを介したCisco NGFWの初期導入時に、ローカルDMZの導入に含まれるポリシールールはどれですか。

- A. 許可ip任意
- B. ポリシールールが含まれていない
- C. ip anyを拒否する
- D. ユーザーのみがIPアドレスを変更できるデフォルトのDMZポリシー。

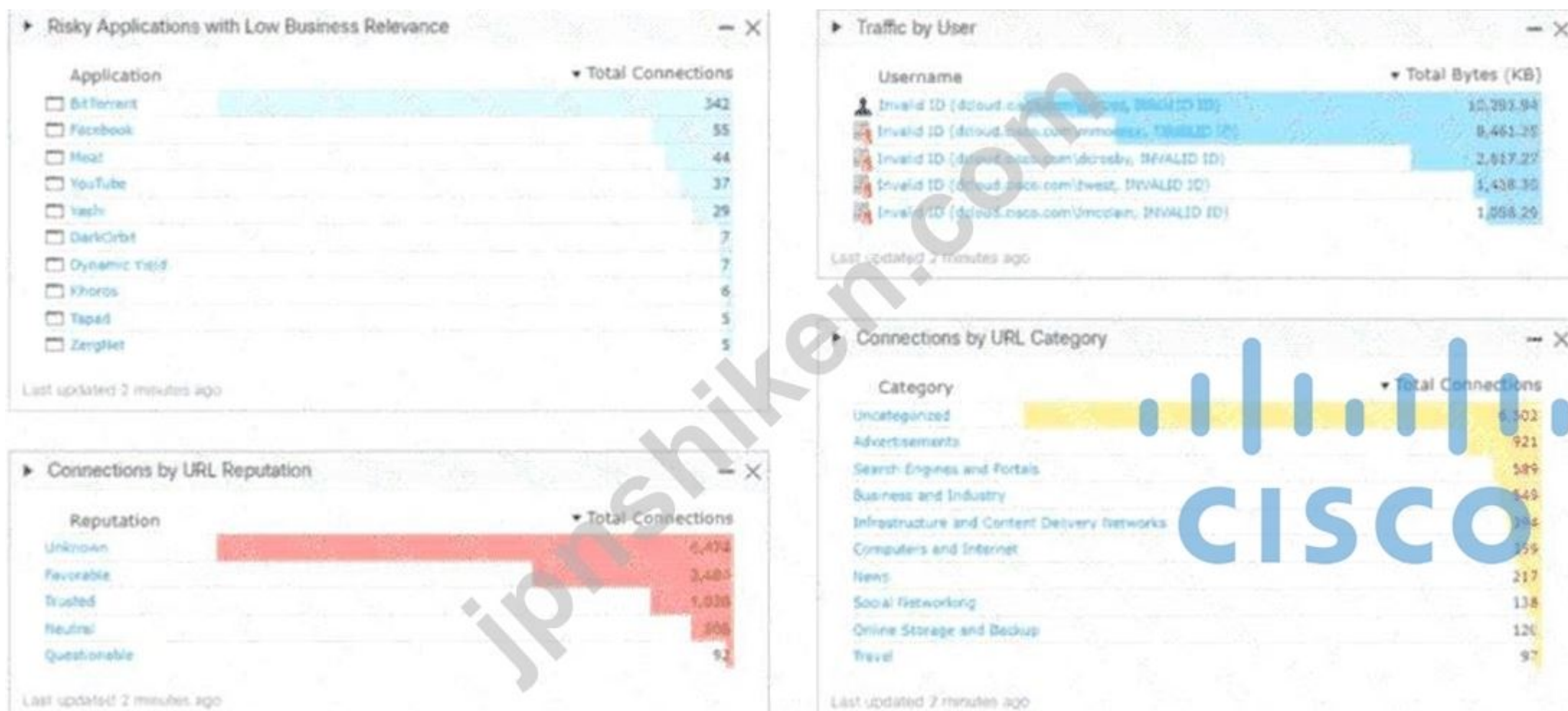
正解: ([正解を表示します](#))

質問: 45

Cisco Secure Firewall Management Center 内の Rapid Threat Containment の修復モジュールとして機能しているのはどれですか？

- A. 適応型ネットワーク制御
- B. Cisco Secure Endpoint
- C. Cisco Identity Services Engine
- D. ネットワーク保護サービス

正解: ([正解を表示します](#))



図を参照してください。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軽減するために、ユーザーはどのような行動を取る必要がありますか？

- A. Dropboxの使用をブロックします。
- B. 評判が不明なすべてのURLを停止します。
- C. すべてのBitTorrentアプリケーションをブロックします。
- D. 分類されていないすべてのURLを停止します。

正解: D ([コメントを发表する](#))

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

エンジニアは、Cisco Secure Firewall Management Centerで、デフォルトですべてのトラフィックをブロックする基本的なアクセス制御ポリシーを作成する必要があります。左側の設定アクションを右側にドラッグアンドドロップして、順番に並べ替えてください。



正解:



質問: 48

Cisco FMC を使用して迅速な脅威の封じ込めを実行するには、どのコンポーネントが必要ですか？

- A. ISE
- B. RESTful API
- C. SIEM
- D. DDI

正解: (正解を表示します)

To perform rapid threat containment with Cisco FMC, the necessary component is Cisco Identity Services Engine (ISE). ISE integrates with FMC to provide dynamic network access control and enforcement, allowing for quick isolation of compromised endpoints based on security events detected by FMC.

Steps:

- * Integrate FMC with ISE by configuring the necessary settings in both platforms.
- * Define security policies in FMC that trigger rapid threat containment actions via ISE.
- * When a threat is detected, FMC can instruct ISE to isolate the affected endpoint, limiting its access to the network.

This integration enables automated and efficient threat containment, reducing the response time and mitigating the impact of security incidents.

References: Cisco Secure Firewall Management Center Integration Guide, Chapter on ISE Integration for Rapid Threat Containment.

質問: 49

ネットワーク管理者はCiscoIPSアプライアンスを導入しており、トラフィックフローに影響を与えることなく最初に動作する必要があります。
また、データを収集して、不要なトラフィックをドロップするように再構成する前に、そのベースラインを提供する必要があります。これらの要件を満たすCiscoIPSモードはどれですか。

- A. インラインタップ
- B. 無差別
- C. バイパス
- D. フェイルセーフ

正解: ([正解を表示します](#))

質問: 50

FTDユニットでどのコマンドを実行して、IPアドレス10.0.0.10にあり、登録キーCisco123を持つFMCマネージャーにユニットを関連付けますか？

- A. ローカル10.0.0.10 Cisco123マネージャーの構成
- B. configure manager add Cisco123 10.0.0.10
- C. ローカルのCisco123 10.0.0.10マネージャーを構成する
- D. configure manager add 10.0.0.10 Cisco123

正解: ([正解を表示します](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

質問: 51

エンジニアが初めて Cisco Secure Endpoint を MAC アドレス 50:54 のエンドポイントに導入しています。
15:04:0:AB。エンジニアは、テストフェーズ中にファイルが分離されておらず、ネットワーク接続がブロックされていないことを確認する必要があります。
このタスクを実行するには、どのタイプのポリシーを設定する必要がありますか？

- A. 監査
- B. 保護
- C. 隔離
- D. トリアージ

正解: ([正解を表示します](#))

質問: 52

組織では、インターネットに送信されるリンクで多くのトラフィックの輻輳が発生しています。企業を離れる前にインターネットに送信されるすべてのトラフィックを処理するCiscoFirepowerデバイスがあります。正当なビジネストラフィックが目的地に到達するように、輻輳はどのように緩和されますか？

- A. 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
- B. QoSポリシーのレート制限高帯域幅アプリケーションを作成します
- C. アプリケーション対応の帯域幅制限にWCCPを使用するflexconfigポリシーを作成します
- D. CiscoFirepowerデバイスが多くのアドレスを変換する必要があるようにNATポリシーを作成します

正解: ([正解を表示します](#))

質問: 53

エンジニアはCisco Secure Firewall Threat Defenseアプライアンスの断続的な接続問題をトラブルシューティングしており、24時間分のデータを収集する必要があります。エンジニアはパケットキャプチャを開始しましたが、キャプチャ中に途中で停止してしまいました。エンジニアは、パケットキャプチャのバッファサイズがデフォルトの32MBに設定されていることに気がきました。パケットキャプチャを正常に実行するためにエンジニアが設定する必要がある最大のバッファサイズはどれでしょうか？

- A. 1GB
- B. 10GB
- C. 64 MB
- D. 100GB

正解: B (コメントを发表する)

質問: 54

ネットワークエンジニアがCisco Firepower 4100アプライアンスを導入し、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にドラッグアンドドロップして、この構成を順番に実行してください。

Add a MAC pool prefix and view the MAC addresses for the container instance interfaces

Configure interfaces

Add a high-availability pair

Add a resource profile for container instances

Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center

1

2

3

4

5

正解:

Add a MAC pool prefix and view the MAC addresses for the container instance interfaces

Configure interfaces

Add a high-availability pair

Add a resource profile for container instances

Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center

Add a resource profile for container instances

Add a MAC pool prefix and view the MAC addresses for the container instance interfaces

Configure interfaces

Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center

Add a high-availability pair

Explanation:

The correct sequence of actions for configuring a multi-instance environment for high availability on a Cisco Firepower 4100 appliance is as follows:

Add a resource profile for container instances. A resource profile defines the CPU, RAM, and disk space allocation for each container instance. You can create multiple resource profiles with different resource settings and assign them to different container instances1.

Add a MAC pool prefix and view the MAC address for the container instance interfaces. A MAC pool prefix is a 24-bit prefix that is used to generate MAC addresses for the container instance interfaces. You can specify a custom MAC pool prefix or use the default one. You can also view the MAC addresses that are assigned to each container instance interface1.

Configure interfaces. You need to configure the physical interfaces, EtherChannels, and VLAN subinterfaces that will be used by the container instances. You can also configure shared interfaces that can be used by multiple container instances on the same security module/engine1.

Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center. You need to add a logical device that runs a standalone Firepower ThreatDefense (FTD) application instance and register it with the Cisco Secure Firewall Management Center (FMC). This logical device will act as the management interface for the container instances1.

Add a high-availability pair. You need to add another logical device that runs a standalone FTD application instance and register it with the FMC as well. Then, you need to configure high availability (HA) between the two standalone FTD logical devices. This will enable HA for the container instances that are associated with them1.

質問: 55

ネットワーク管理者は、リモートアクセスVPNユーザーがネットワーク内から到達できないことに気づきました。ルーティングが正しく構成されていると判断されましたが、リターントラフィックはファイアウォールに入っていますが、ファイアウォールから出ていません。この問題の理由は何ですか。

- A. 手動のNAT免除ルールがNATテーブルの先頭に存在しません。
- B. 外部NATIPアドレスが構成されていません。
- C. 外部NATIPアドレスが間違ったインターフェースに一致するように構成されています。
- D. オブジェクトNAT免除ルールがNATテーブルの先頭に存在しません。

正解: **A** ([コメントを发表する](#))

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html>

質問: 56

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 サーバへの HTTP トラフィックをトラブルシューティングしています。キャプチャを確認すると、エンジニアは、キャプチャされた Web サーバーから送信されたものでも送信されたものでもないパケットが多数あることに気付きます。エンジニアは、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どのように軽減できますか？

- A. パケット キャプチャ内でアクセス 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。
- B. -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。
- C. パケット キャプチャでホスト フィルタを使用して、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。
- D. パケット キャプチャの出力を、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。

正解: ([正解を表示します](#))

質問: 57

ある組織は、IPS機能のないCisco Firepowerを導入しましたが、トラフィックの検査を有効にしたいと考えています。プロトコルの異常を検出し、Snort ルールセットを使用して悪意のある動作を検出できるようにする必要があります。これはどのように実現できますか？

- A. ネットワーク分析ポリシーを変更して、検査対象のパケットを処理する
- B. アクセス制御ポリシーを変更して、興味深いトラフィックをエンジンにリダイレクトします。
- C. 検査対象となる新しいホストを検出するために、ネットワーク検出ポリシーを変更します。

D. 侵入ポリシーを変更して、検査対象となるイベントの最小深刻度を決定します。

正解: D ([コメントを发表する](#))

質問: 58

エンジニアは、Cisco Secure IPSデバイスをパッシブモードを使用してトラフィックを監視するようにSPANを設定する必要があります。

Cisco Secure IPSインターフェイスGi0/1は、Cisco CatalystスイッチインターフェイスGi0/3に接続されています。どのSPAN構成が要件を満たしますか？

A.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source interface Gi0/3
Switch(config)# monitor session 1 destination interface Gi0/3
Switch(config)# end
```

B.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor source interface Gi0/1
Switch(config)# monitor destination interface Gi0/3
Switch(config)# end
```

C.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor source interface Gi0/1
Switch(config)# monitor destination interface Gi0/1
Switch(config)# end
```

D.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source interface Gi0/1
Switch(config)# monitor session 1 destination interface Gi0/3
Switch(config)# end
```

正解: D ([コメントを发表する](#))

In a local SPAN configuration, the source is the switch interface whose traffic must be copied, while the destination is the interface connected to the passive monitoring device. Therefore, switch interface Gi0/1 must be configured as the SPAN source, and switch interface Gi0/3, which connects to the Cisco Secure IPS sensor, must be the destination. Both commands must also reference the same SPAN session number. Option D satisfies all these requirements. Options B and C omit the mandatory session number, while Option A incorrectly assigns Gi0/3 as both the source and destination. A SPAN destination cannot simultaneously be a source in the same session. The passive IPS receives the mirrored packets for inspection but does not retransmit or directly block them. Cisco SPAN configuration documentation

質問: 59

ネットワーク管理者が月次の高度なマルウェアリスクレポートを確認している際に、CnC接続済みとしてリストされているホストに気づきました。このホストがマルウェアに感染しているかどうかをさらに確認するには、Cisco FMCのどこを調べればよいでしょうか？

- A. 分析 > ホスト > 侵害の兆候
- B. アナリスト > ファイル > マルウェアイベント
- C. 分析 > ホスト > ホスト属性
- D. 分析 > フライ > ネットワークファイル軌跡

正解: ([正解を表示します](#))

To determine if a host is infected with malware, the network administrator can look at the Indications of Compromise (IOC) feature in Cisco FMC. The IOC feature analyzes network and endpoint data collected by Firepower sensors and AMP for Endpoints connectors, and identifies hosts that exhibit signs of compromise or infection. The IOC feature uses predefined rules based on Cisco Talos intelligence and other sources to detect IOCs on hosts. One of these rules is CnC Connected, which indicates that a host has communicated with a command-and-control (CnC) server that is known to be associated with malware activity².

To view the IOC information for a host, the network administrator can navigate to Analysis > Hosts > Indications of Compromise in Cisco FMC, and select a host from the table. The IOC Details page will show the IOC events for that host, including the CnC Connected event, along with other information such as severity, timestamp, source, destination, protocol, and rule name. The network administrator can also view more details about each IOC event by clicking on it².

The other options are incorrect because:

Analysis > Files > Malware Events shows information about files that have been detected as malware by Firepower sensors or AMP for Endpoints connectors. This does not show information about hosts that are infected with malware or have communicated with CnC servers³.

Analysis > Hosts > Host Attributes shows information about hosts that have been discovered by Firepower sensors, such as IP address, MAC address, operating system, applications, users, vulnerabilities, and so on. This does not show information about IOCs or CnC connections on hosts⁴.

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

質問: 60

ネットワーク管理者は、Cisco Secure Firewall Management Centerで管理されているCisco Secure Firewall Threat Defenseデバイスを、上流のBGPルータとルーティング情報を交換するように設定しています。管理者は、デバイスが上流ルータにアドバタイズしているネットワークを確認する必要があります。管理者はどのような操作を行う必要がありますか？

- A. 詳細トラブルシューティングから show bgp neighbors NEIGHBOR-IP advertised-routes コマンドを実行します。
- B. セキュアファイアウォール脅威防御デバイスのデバイスルーティング設定で ルートインジェクション」を選択します。
- C. Secure Firewall Management Center のデバイスルーティング設定で、[ルートインジェクション] を選択します。
- D. Secure Firewall Management Center CLI から show route コマンドを実行します。

正解: A ([コメントを发表する](#))

The show bgp neighbors NEIGHBOR-IP advertised-routes command displays the prefixes that the Secure Firewall Threat Defense device is advertising to a specific BGP neighbor. It must be executed against the managed threat defense device through the Advanced Troubleshooting interface. The ordinary show route command displays routes installed in the local routing table, not the specific prefixes advertised to a neighbor.

Route injection is a configuration capability and does not provide the required verification output. Cisco's command reference confirms that the advertised-routes keyword displays all routes advertised to the specified BGP peer, including the network, next hop, metric, weight, and AS path. Therefore, option A directly verifies the routes being shared with the upstream router. Cisco Secure Firewall Threat Defense Command Reference

質問: 61

ネットワーク管理者は、Cisco Secure Firewall Management Centerで管理されているCisco Secure Firewall Threat Defenseインスタンスを構成して、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したいと考えています。この要件を満たすために、管理者はSecure Firewall Management Centerでどのシステム設定を構成する必要がありますか？

- A. アクセス ポリシー。セキュリティ インテリジェンス
- B. マルウェア対策ポリシー
- 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

正解: ([正解を表示します](#))

To block traffic to known cryptomining networks using Cisco Secure Firewall Threat Defense (FTD) managed by Cisco Secure Firewall Management Center (FMC), the network administrator needs to configure Security Intelligence in an Access Control Policy. Security Intelligence allows administrators to block traffic based on threat intelligence feeds, which include known malicious IP addresses, domains, and URLs.

Steps:

Navigate toPolicies > Access Control > Access Control Policyin FMC.

Edit or create an Access Control Policy.

Go to theSecurity Intelligencetab.

Enable the relevant threat intelligence feeds that include cryptomining networks.

Apply the policy to the FTD device.

This configuration ensures that traffic to known cryptomining networks is blocked, enhancing the network ' s security posture against cryptomining threats.

References:Cisco Secure Firewall Management Center Configuration Guide, Chapter on Security Intelligence.

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 62

Cisco FTD統合ルーティングおよびブリッジングでは、ブリッジグループはルーティングされたインターフェイスとの通信にどのインターフェイスを使用しますか。

- A. 仮想スイッチ
- B. ブリッジグループメンバー
- C. 仮想ブリッジ
- D. サブインターフェース

正解: ([正解を表示します](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

質問: 63

Cisco FMCへのデバイスの削除と再追加に関する記述のうち、正しいものはどれですか？(2つ選択してください。)

- A. 登録時に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、ユーザーは登録完了後にポリシーを再適用する必要はありません。
- B. Cisco FMC にデバイスを再追加する前に、デバイスにマネージャー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追加するオプションは利用できません。
- D. Cisco FMCのWebインターフェースは、ユーザーにアクセス制御ポリシーを再適用するように促します。
- E. 登録時にNATおよびVPNポリシーを再適用するオプションは利用できないため、ユーザーは登録完了後にポリシーを再適用する必要があります。

正解: ([正解を表示します](#))

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

質問: 64

エンジニアが、新しいCisco FTDデバイスの背後にあるホストからDNSサーバーへの接続に関するトラブルシューティングを行っている。ホストはDMZ内のサーバーにDNSクエリを送信できません。エンジニアは、実際のDNSパケットを使用してこの問題をトラブルシューティングするために、どのような対策を講じるべきでしょうか？

- A. パケットトレーサツールを使用して、パケットがどのホップでドロップされているかを特定します。
- B. 接続イベントダッシュボードを使用してブロック理由を確認し、必要に応じて検査ポリシーを調整します。
- C. Threat Defense CLI ツールで show blocks コマンドを使用し、ブロックされたトラフィックを許可するポリシーを作成します。
- D. パケットキャプチャツールを使用して、トラフィックがどこでブロックされているかを確認し、必要に応じてアクセス制御または侵入ポリシーを調整します。

正解: B ([コメントを发表する](#))

質問: 65

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

- A. モニター
- B. ブロック
- C. インタラクティブブロック
- D. 警告付きで許可

正解: ([正解を表示します](#))

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

質問: 66

IRB モードの Cisco FTD デバイスでダイナミック ルーティング プロトコルを実行するときに考慮すべき制限は何ですか？

- A. リンクが古いルーティング プロトコルのみがサポートされます。
- B. ディスタンス ベクトル ルーティング プロトコルのみがサポートされます。
- C. EtherChannel インターフェイスのみが想定されます。
- D. 非ブリッジインターフェイスのみがサポートされます。

正解: **D** ([コメントを發表する](#))

Integrated routing and bridging (IRB) is a feature that allows you to route between different bridge groups on a Cisco FTD device. A bridge group is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. You can assign an IP address to a bridge group interface (BVI) and enable routing protocols on it, just like a regular routed interface. However, when you run a dynamic routing protocol on a Cisco FTD device in IRB mode, you can only use nonbridge interfaces as routing peers. You cannot use bridge group interfaces or bridge group member interfaces as routing peers². This is because the routing protocol packets are sent and received on the nonbridge interfaces, and the bridge group interfaces are used only for forwarding data traffic³.

質問: **67**

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

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

正解: ([正解を表示します](#))

質問: **68**

高可用性をサポートする2つの展開タイプはどれですか？ 2つ選択してください。)

- A.** 透明
- B.** ルーティング
- C.** クラスター化
- D.** シャーシ内マルチインスタンス
- E.** パブリッククラウドの仮想アプライアンス

正解: **A,B** ([コメントを發表する](#))

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

質問: **69**

ある企業は、Cisco FMCによって管理される多数の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、アクセス制御ルールのログを収集して分析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に対してCisco FMCが処理能力不足になる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、どの構成が適切でしょうか？

- A.** Cisco FTD接続イベントをSIEMシステムに直接送信し、Cisco FMCからのセキュリティイベントをSIEMシステムに転送して保存および分析します。
- B.** Cisco FTD の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構成します。
- C.** Cisco FTDの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て保存および分析します。
- D.** Cisco FTDの接続イベントとセキュリティイベントを、保存と分析のためにCisco FMCデバイスのクラスタに送信します。

正解: **B** ([コメントを發表する](#))

質問: 70

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

- A. ベース
- B. モビリティ
- C. 頂点
- D. プラス

正解: D ([コメントを发表する](#))

質問: 71

エンジニアが、会社の財務データに追加の保護を提供するため、Cisco FTD デバイスを財務 VLAN に配置するように設定しています。このデバイスは、現在 DHCP を使用して IP アドレスを取得しているエンドユーザーのワークステーションに変更を加えることなく展開する必要があります。この要件を満たすために、エンジニアはどのようにデバイスを展開する必要がありますか？

- A. デバイスをルーティングモードで展開し、アクセス制御ポリシーでDHCPトラフィックを許可します。
- B. デバイスをルーティングされた場所に展開して、DHCPリレー機能を有効にします。
- C. デバイスを透過モードで展開し、アクセス制御ポリシーでDHCPトラフィックを許可する。
- D. デバイスを透過モードで展開し、DHCPサーバー機能を有効にします。

正解: ([正解を表示します](#))

Transparent mode allows the FTD device to act as a "bump in the wire" that does not affect the IP addressing of the network. The end user workstations will not need any changes to their configuration, as they will still receive an IP address from the same DHCP server. However, the FTD device must allow DHCP traffic in the access control policies, otherwise it will block the DHCP requests and replies1

質問: 72

Cisco Firepowerデバイスを介して通信しているクライアントとサーバ間で接続の問題が発生していますトラブルシューティング中に、ネットワーク管理者はトラフィックがサーバに到達していることを確認しましたが、クライアントは応答を受け取りませんこの問題を解決するにはどの手順を実行する必要がありますかクライアントからのトラフィックを開始せずに？

- A. パケットトレーサーを使用して、パケットがファイアウォールを通過し、修正されたIPアドレスにNATされていることを検証します。
- B. パケットキャプチャを使用して、パケットがファイアウォールを通過し、修正されたIPアドレスにNATされていることを検証します。
- C. パケットキャプチャを使用して、トラフィックがアクセスリストによってブロックされていないことを確認します。
- D. パケットトレーサーを使用して、トラフィックがアクセスリストによってブロックされていないことを確認します。

正解: ([正解を表示します](#))

質問: 73

セキュリティエンジニアが、Cisco Secure Firewall Management Center のサマリーダッシュボードにインターフェイストラフィックウィジェットを追加しようとしています。エンジニアは [ウィジェットの追加] をクリックして編集モードに入ります。設定を完了するために、セキュリティエンジニアはどのような操作を行う必要がありますか？

- A. すべてのカテゴリ」をクリックし、 分析とレポート」タブを開いてから、 ウィジェットを追加」ボタンをクリックします。
- B. すべてのカテゴリ」をクリックし、 新規」タブを開いてから、 ウィジェットを追加」ボタンをクリックします。
- C. すべてのカテゴリ」をクリックし、 操作」タブを開いてから、 ウィジェットを追加」ボタンをクリックします。

D. すべてのカテゴリ」をクリックし、その他」タブを開いてから、ウィジェットを追加」ボタンをクリックします。

正解: [\(正解を表示します\)](#)

The Interface Traffic widget belongs to the Operations category because it displays operational information about appliance interfaces, specifically received and transmitted traffic rates. After selecting Add Widgets, the engineer can select All Categories and open Operations to locate Interface Traffic, then click Add next to the widget. Analysis & Reporting contains widgets based on collected security events and analytical data.

Miscellaneous contains widgets that display neither event nor operational data, such as the RSS Feed widget.

"New" is not a valid predefined widget category. Cisco classifies Operations widgets as those that display system status and overall health information. The Interface Traffic widget is not included on predefined dashboards by default, so it must be added manually using this procedure. Cisco Secure Firewall dashboard documentation

質問: 74

エンジニアは、CiscoFMCでURLオブジェクトを定義する必要があります。SSLインスペクションを実行せずにURLを指定する正しい方法は何ですか？

- A. サブジェクト共通名の値を使用します。
- B. オブジェクトグループ内のすべてのサブドメインを指定します。
- C. オブジェクトのプロトコルを指定します。
- D. CRL配布ポイントからのすべてのURLを含めます。

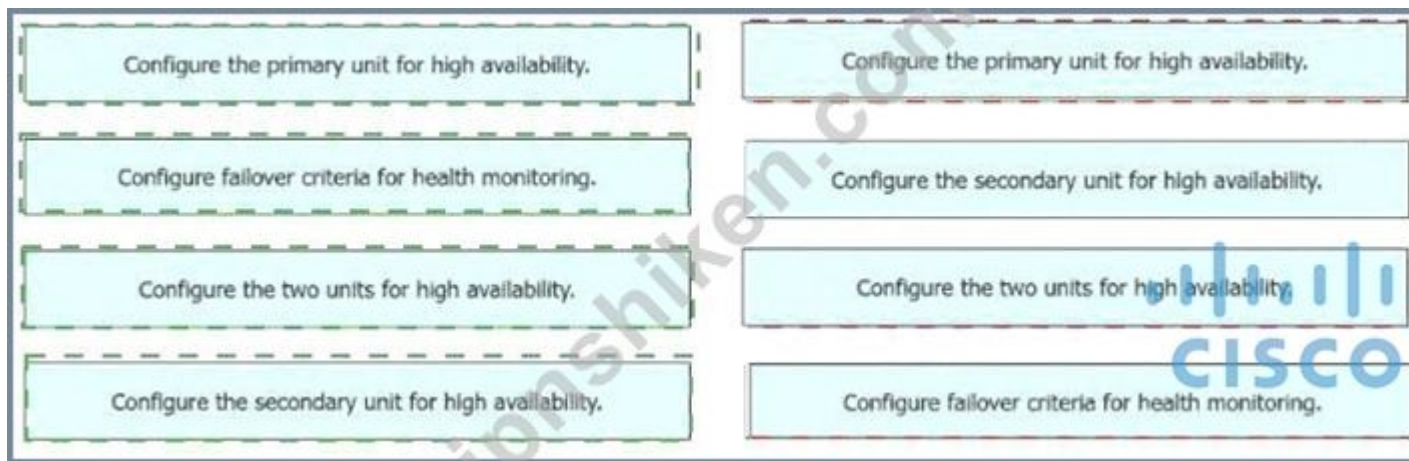
正解: B [\(コメントを發表する\)](#)

質問: 75

エンジニアは、2台のCisco Secure Firewall Threat Defenseアプライアンスで高可用性を構成する必要があります。左側の構成手順を右側の順序にドラッグアンドドロップしてください。

Configure the primary unit for high availability.	step 1
Configure failover criteria for health monitoring.	step 2
Configure the two units for high availability.	step 3
Configure the secondary unit for high availability.	step 4

正解:



Explanation:

Step 1(Configurate the primary unit for high availability),

Step 2(Configurate the secondary unit for high availability),

Step 3(Configurate the two units for high availability),

Step 4(Configurate failover criteria for health monitoring)

質問: 76

Cisco Secure Firewall Threat Defense デバイスでパケットキャプチャを使用し、パケットフローがマルウェアクエリに対して激しく反応している場合、Snort の判定結果はどれになりますか？

A. 再試行

B. 置き換える

C. ブロック

D. ブロックフロー

正解: (正解を表示します)

When packet capture is used on a Cisco Secure Firewall Threat Defense (FTD) device and the packet flow is waiting on the malware query, the Snort verdict appears as " retry. " This indicates that the device is still processing the malware analysis and has not yet determined the final action for the packet. The " retry " verdict signifies that the packet is in a holding state while awaiting the result of the malware inspection, which helps in maintaining the security posture until a definitive decision is made.

References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Packet Capture and Malware Inspection.

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 77

エンジニアは、Cisco FMC でリモートストレージを設定する必要があります。構成のバックアップは、災害復旧のためにネットワーク上の安全な場所から入手できる必要があります。レポートは、監査人が Active Directory ログインでアクセスできる共有の場所にバックアップする必要があります。これらの目標を達成するために、エンジニアはどの戦略を使用する必要がありますか？

A. バックアップには SMB を使用し、レポートには NFS を使用します。

- B. バックアップとレポートの両方に NFS を使用します。
- C. バックアップとレポートの両方に SMB を使用します。
- D. バックアップには SSH を使用し、レポートには NFS を使用します。

正解: ([正解を表示します](#))

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/system_configuration.html#ID-2241-00000551

"You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

質問: 78

一定期間に受信するイベントの数を減らすために使用されるCisco Firepower機能はどれですか。

- A. レート制限
- B. 一時停止
- C. 相関
- D. しきい値処理

正解: ([正解を表示します](#))

Reference: <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.html>

質問: 79

組織のCEOからのネットワークトラフィックのコイニングは決して否定されてはなりません。展開エンジニアがすべてのトラフィックを許可するルールを作成することを許可されていない場合、どのアクセス制御ポリシー構成オプションを使用する必要がありますか？

- A. ファイアウォールバイパスを構成します。
- B. CEOの信頼ポリシーを構成します。
- C. 侵入ポリシーをセキュリティからバランスに変更します。
- D. CEO専用のNATポリシーを作成します。

正解: ([正解を表示します](#))

質問: 80

展示資料を参照してください。

システム管理者がホストマシンからSCCMサーバーへの接続テストを実行したところ、サーバーから応答がありませんでした。pingパケットが宛先に到達し、ホストが応答を受信することを確実にするには、どの操作を行うべきでしょうか？

- A. 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。
- B. 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。
- C. Snort ルールを変更して ICMP トラフィックを許可します。
- D. ICMP許可リストを作成し、ICMP宛先を追加して暗黙の拒否リストから削除します。

正解: ([正解を表示します](#))

質問: 81

ネットワークエンジニアは、脅威検出を強化するためにサードパーティの脅威フィードをCisco FMCに追加したいと考えています。この目標を達成するには、どのアクションを実行する必要がありますか。

- A. STIXとTAXIIを使用して迅速な脅威の封じ込めを有効にする
- B. RESTAPIを使用してThreatIntelligenceDirectorを有効にする
- C. RESTAPIを使用して迅速な脅威の封じ込めを有効にする
- D. STIXおよびTAXIIを使用してThreat IntelligenceDirectorを有効にする

正解: ([正解を表示します](#))

質問: 82

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. ヘルス モニター ページにアクセスします。
- B. 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。
- C. ヘルス イベント ページにアクセスします。
- D. 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。
- E. Secure Firewall Threat Defense デバイスのプロパティを選択します。

正解: ([正解を表示します](#))

質問: 83

エンジニアは HTTP トラフィック用のカスタム アプリケーション ディテクタを構成しており、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タイプのハエとして作成し、アップロードしますか？

- A. Perlスクリプト
- B. NBARプロトコル
- C. LUA スクリプト
- D. Python プログラム

正解: **C** ([コメントを发表する](#))

A custom application detector is a user-defined script that can detect web applications, clients, and application protocols based on patterns in network traffic. Custom application detectors are written in LUA, which is a lightweight and embeddable scripting language. LUA scripts can use predefined functions and variables provided by the Firepower System to access packet data and metadata, and to specify the detection criteria and the application information¹.

To import a custom application detector file that was provided by a third party, you need to follow these steps¹:

- * In the FMC web interface, navigate to Objects > Object Management > Application Detectors.
- * Click Import.
- * Browse to the location of the LUA script file and select it.
- * Click Upload.
- * Review the detector details and click Save.

The other options are incorrect because:

- * Perl script is not a supported format for custom application detectors. Perl is a general-purpose programming language that is not embedded in the Firepower System.

* NBAR protocol is not a file type, but a feature of Cisco IOS routers that can classify and monitor network traffic based on application types. NBAR protocols are predefined and cannot be imported as custom application detectors.

* Python program is not a supported format for custom application detectors. Python is a general-purpose programming language that is not embedded in the Firepower System.

質問: 84

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

- A. 両方の部門にパッシブIDSポートを使用する
- B. 両方の部門にTAPモードで設定された1組のインラインを使用します
- C. 論理トラフィックの分離を維持するためにVLANで802.1Q mimesetトランクインターフェイスを使用する
- D. 各部門に専用のIPSインラインセットを使用して、トラフィックの分離を維持します

正解: ([正解を表示します](#))

質問: 85

エンジニアが、Cisco Secure Firewall Management Centerで管理されているCisco Secure Firewall Threat Defenceデバイスを設定しています。このデバイスでは、リモート管理のためにSSHが有効になっており、内部インターフェイスからアクセス可能である必要があります。エンジニアは、これを実現するためにどのタイプのポリシーを設定する必要がありますか？

- A. 識別する
- B. アクセス制御
- C. プレフィルタ
- D. プラットフォーム設定

正解: ([正解を表示します](#))

To enable SSH access to a Cisco Secure Firewall Threat Defense (FTD) device from the inside interface for remote administration, the engineer needs to configure a Platform Settings policy in Cisco Secure Firewall Management Center (FMC). The Platform Settings policy allows the configuration of various system-related settings, including enabling SSH, specifying the allowed interfaces, and defining the SSH access parameters.

Steps:

In FMC, navigate to Policies > Access Control > Platform Settings.

Create a new Platform Settings policy or edit an existing one.

In the policy settings, go to the SSH section.

Enable SSH and specify the inside interface as the allowed interface for SSH access.

Define the SSH parameters such as allowed IP addresses, user credentials, and other security settings.

Save and deploy the policy to the FTD device.

This configuration ensures that SSH access is enabled on the specified interface, allowing secure remote administration.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings.

質問: 86

エンジニアは、パッシブモードのCisco Secure IPSデバイスを使用してトラフィックを監視するために、SPANセッションを設定する必要があります。Cisco Secure IPSインターフェイスGi0/1は、Cisco CatalystスイッチインターフェイスGi0/3に接続されています。どのSPAN構成が要件を満たしますか？

A. Switch(config)# monitor source interface Gi0/1

Switch(config)# monitor destination interface Gi0/3

B. Switch(config)# monitor session 1 source interface Gi0/3

Switch(config)# monitor session 1 destination interface Gi0/3

C. Switch(config)# monitor session 1 source interface Gi0/1

Switch(config)# monitor session 1 destination interface Gi0/3

D. Switch(config)# monitor source interface Gi0/1

Switch(config)# monitor destination interface Gi0/3

正解: ([正解を表示します](#))

A local SPAN configuration requires a numbered monitoring session with a source interface and a different destination interface. Gi0/1 is the switch interface whose traffic must be copied, while Gi0/3 is connected to the passive Cisco Secure IPS sensor and must therefore be the SPAN destination.

Option C correctly associates both commands with session 1 and maps the monitored traffic from Gi0/1 to Gi0/3. Option B incorrectly makes Gi0/3 both the source and destination, which cannot provide the required monitoring path.

Options A and D omit the mandatory session 1 portion of the Catalyst SPAN syntax. Because the IPS operates passively, it receives copies of packets on its monitoring interface without becoming an inline forwarding device and without being able to disrupt the production traffic.

質問: 87

管理対象デバイスをインラインで展開するための最小要件は何ですか？

A. インラインインターフェイス、セキュリティゾーン、MTU、モード

B. パッシブインターフェイス、MTU、モード

C. インラインインターフェイス、MTU、モード

D. パッシブインターフェイス、セキュリティゾーン、MTU、モード

正解: **C** ([コメントを发表する](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html

質問: 88

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

A. 問題のデバイスの \$showtech」ファイル。

B. CiscoFMCの 「ショーテック」。

C. 問題のデバイスの 「トラブルシューティング」ファイル。

D. CiscoFMCの 「トラブルシューティング」ファイル。

正解: ([正解を表示します](#))

質問: 89

Cisco Rapid Threat Containment がネットワーク内の脅威を封じ込めるために使用する方法は何ですか？

A. TACACS+

B. コンテキストデータの共有

C. 認証の変更

D. トラストセグメンテーション

正解: ([正解を表示します](#))

質問: 90

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

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

正解: ([正解を表示します](#))

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf>

質問: 91

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

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

正解: ([正解を表示します](#))

A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take when it encounters different types of files. The file policy is applied as part of an access control policy. If an access control policy does not include a file policy, the FTD device will not take any action on the files it encounters, resulting in a disposition of " unknown " for all file types except exe.

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-cisco-firepow.html>

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 92

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

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

正解: ([正解を表示します](#))

質問: 93

エンジニアは、CiscoFTDセンサーの設定をプルしてCiscoTACで確認しようとしませんが、デバイスのCUIに直接アクセスすることはできません。デバイスのCL1は、エンジニアがアクセスできるCiscoFMCによって管理されます。Cisco FMCのどのアクションが、デバイスのCL1へのアクセスを許可しますか。

- A. CiscoFMC内のCiscoFTDCLI機能でshowrunallコマンドを使用します。
- B. CiscoFMC内のインポート/エクスポートツールを使用して設定をエクスポートします。
- C. CiscoFMCの[FileDownload]セクションで設定ファイルをダウンロードします。
- D. CiscoFMC内に設定のバックアップを作成します。

正解: ([正解を表示します](#))

質問: 94

Cisco Secure Firewall Threat Defence デバイスは、インライン IPS モードに設定され、インライン セット内のインターフェイスを通過するすべてのトラフィックを検査します。VDB アップデートの適用中にトラフィックが中断されずに通過できるようにするには、インライン セット設定のどの項目を接続する必要がありますか？

- A. リンク状態を伝播する
- B. ショートフォールオープン
- C. 厳格なTCP強制
- D. タップモード

正解: ([正解を表示します](#))

In inline IPS mode, to ensure that traffic passes through uninterrupted when VDB (Vulnerability Database) updates are being applied, the " Short Fall Open " setting must be configured. This setting allows traffic to continue to flow through the firewall even if there are issues with the inspection process, such as during updates or if the inspection engine fails.

Steps:

In FMC, navigate to the inline set configuration.

Enable the " Short Fall Open " option.

Deploy the configuration to the FTD device.

This ensures that network traffic is not disrupted during updates or other issues with the inspection process.

References:Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Inline IPS Mode Configuration.

質問: 95

Cisco FMC Webインターフェイス内のどの機能で、ネットワークトラフィック内のマルウェアを検出、分析、およびブロックできますか。

- A. file policies
- B. Cisco AMP for Networks
- C. Cisco AMP for Endpoints
- D. intrusion and file events

正解: B ([コメントを發表する](#))

質問: 96

図を参照してください。



既存の Cisco FMC 構成の影響は何ですか？

- 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 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。
- 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. Cisco FMC と Cisco FTD 間の管理接続が無効になります。

正解: **D** ([コメントを发表する](#))

質問: 97

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

- A. 接続されたデバイスのデフォルトゲートウェイとしてBVIIPアドレスを指定します。
- B. CiscoFirepowerでルーティングを有効にします
- C. 物理CiscoFirepower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構成します。

正解: ([正解を表示します](#))

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each

other.<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general>

[/asa-97-general-config/intro-fw.html](#)

質問: 98

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まとめられるのでしょうか？

- A. マルウェアレポートを生成します。

- B. カスタムレポートを作成します。
- C. デフォルトのFirepowerレポートを実行します。
- D. 攻撃リスクレポートをエクスポートします。

正解: ([正解を表示します](#))

質問: 99

図を参照してください。



エンジニアは、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。正常に完了したタスクは、ファイルがダウンロードされる前に削除されます。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. Secure FMC のエキスパート モードに FTP クライアントを使用して、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] をクリックして、ファイル名を入力し、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 モードに移動します。/var/common の内容を一覧表示し、出力から正しいファイル名を特定します。
- E. [システム モニタリング]、[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特定します。

正解: ([正解を表示します](#))

If a task to generate troubleshooting files in Cisco Secure Firewall Management Center (FMC) is completed successfully but removed before the files are downloaded, the following steps can be taken to determine the filename and obtain the generated troubleshooting files without regenerating them:

Go to expert mode on Secure FMC:

Access expert mode on the FMC via SSH or the console.

List the contents of the directory/var/common to locate the generated troubleshooting files. Use the commandls /var/common.

Use the System Monitoring Audit logs:

In FMC, navigate toSystem > Monitoring > Audit.

Find the line containing the " Generate Troubleshooting Files " string to determine the correct filename.

These actions help identify and retrieve the generated troubleshooting files without the need to regenerate them, saving time and resources.

References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Troubleshooting and File Management.

質問: 100

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

- A. URLソースを追加し、CiscoFMC内でフラットファイルタイプを選択します。
- B. txtファイルをSTIXに変換し、CiscoFMCにアップロードします。
- C. 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。

D. TAXIIフィードソースを追加し、フィードのURLを入力します。

正解: ([正解を表示します](#))

質問: 101

トラブルシューティングファイルを生成するために、Cisco FMC CLIでどのコマンドを入力しますか？

- A. show running-config
- B. show tech-support chassis
- C. system support diagnostic-cli
- D. sudo sf_troubleshoot.pl

正解: ([正解を表示します](#))

Reference: <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html>

質問: 102

管理者は、拡張子が .exe のマルウェアが存在することに気づき、ネットワーク上のシステムのいずれかが実行可能ファイルを実行しているかどうかを確認する必要があります。このデータを表示するには、Cisco AMP for Endpoints 内で何を構成する必要がありますか？

- A. 蔓延
- B. 脅威の根本原因
- C. ファイル分析
- D. 脆弱なソフトウェア

正解: A ([コメントを發表する](#))

質問: 103

セキュリティ エンジニアは、STIX/TAXII データを含む外部フィードを Cisco FMC と統合する必要があります。この接続をサポートするには、Cisco FMC でどの機能を有効にする必要がありますか？

- A. セキュリティ インテリジェンス フィード
- B. 脅威インテリジェンス ディレクター
- C. Cisco セキュア エンドポイント統合
- D. シスコ サクセス ネットワーク

正解: B ([コメントを發表する](#))

質問: 104

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

- A. in cluster interface mode
- B. in a cluster span EtherChannel
- C. in active/passive mode
- D. in active/active mode

正解: C ([コメントを發表する](#))

質問: 105

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

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

正解: ([正解を表示します](#))

質問: 106

AMPがファイルをマルウェアとして識別したことをCisco Threat Responseが通知した場合、どのアクションを実行する必要がありますか？

- A. テクニカルサポートのためにスナップショットをシスコに送信します。
- B. Cisco Threat Responseがマルウェアを自動的にブロックするのを待ちます。
- C. 調査結果を外部の脅威分析エンジンに転送する。
- D. 悪意のあるファイルをブロックリストに追加します。

正解: ([正解を表示します](#))

有効的な**300-710J**問題集はJPNTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-710J**試験問題集を提供します。JPNTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 107

ネットワークエンジニアは、Cisco Secure Firewall Management Centerのコンソールから脅威イベントを監視する必要があります。エンジニアは、Cisco Secure Firewall Malware DefenseをSecure Firewall Management Centerに統合します。エンジニアは次にどのような操作を行う必要がありますか？

- A. Cisco Secure Endpointにログインし、[許可]をクリックしてSecure Firewall Malware DefenseとSecure FMCの接続を承認し、Secure Firewall Malware Defenseクラウド接続をSecure FMCに追加します。
- 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]をクリックしてSecure Firewall Malware DefenseとSecure FMCの接続を承認します。
- C. Secure Endpointにログインし、[許可]をクリックしてSecure Firewall Malware DefenseとSecure FMCの接続を承認し、Secure FMCにSecure Firewall Malware Defenseクラウド接続を追加し、Secure Endpoint用にSecure Firewall Malware Defenseクラウドを選択します。
- D. Secure FMCでSecure Firewall Malware Defenseクラウド接続を追加し、Secure Endpoint用のSecure Firewall Malware Defenseクラウドを選択し、Secure Endpointにログインして、[許可]をクリックしてSecure Firewall Malware DefenseとSecure FMCの接続を承認します。

正解: **D** ([コメントを发表する](#))

質問: 108

Cisco Firepowerシステムでアクセスコントロールポリシーが機能するのはどの2つの方法ですか？ 2つ選択してください。）

- A. 設定の変更が導入されると、トラフィック検査が一時的に中断される可能性があります。
- B. システムは侵入検査を実行した後、ファイル検査を実行します。
- C. セキュリティインテリジェンスデータに基づいてトラフィックをブロックできます。

- D. ファイルポリシーは、関連する変数セットを使用して侵入防止を実行します。
- E. システムは、信頼できるトラフィックの予備検査を実行して、信頼できるパラメータと一致することを確認します。

正解: ([正解を表示します](#))

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

質問: 109

Cisco FTDアクセス制御ポリシーのどのデフォルトアクション設定では、未定義のアプリケーションからのすべてのトラフィックがSnortによる検査なしで通過できるようになりますか？

- A. すべてのトラフィックを信頼する
- B. 基本ポリシーを継承する
- C. ネットワーク検出のみ
- D. 侵入防止

正解: ([正解を表示します](#))

The default action setting in a Cisco FTD Access Control Policy determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data3.

The Trust All Traffic option allows all traffic from an undefined application to pass without Snort inspection.

This option also disables Security Intelligence filtering, file and malware inspection, and URL filtering for all traffic handled by the default action. This option is useful when you want to minimize the performance impact of access control on your network3.

The other options are incorrect because:

The Inherit from Base Policy option inherits the default action setting from the base policy. The base policy is the predefined access control policy that you use as a starting point for creating your own policies. Depending on which base policy you choose, the inherited default action setting can be different3.

The Network Discovery Only option inspects all traffic for discovery data only. This option enables Security Intelligence filtering for all traffic handled by the default action, but disables file and malware inspection, URL filtering, and intrusion inspection. This option is useful when you want to collect information about your network before you configure access control rules3.

The Intrusion Prevention option inspects all traffic for intrusions and discovery data. This option enables Security Intelligence filtering, file and malware inspection, URL filtering, and intrusion inspection for all traffic handled by the default action. This option provides the most comprehensive protection for your network, but also has the most performance impact3.

質問: 110

アナリストがネットワーク内の侵害の可能性の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. 攻撃を受けたマシンの数、攻撃元、およびトラフィックパターン
- B. 侵入イベント、ホスト接続、ユーザーセッション
- C. 時間の経過に伴う脅威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. ユーザーによる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

正解: ([正解を表示します](#))

質問: 111

ネットワーク管理者は、Cisco Secure Firepower Management Center を使用して、データセンター内の複数のファイアウォールを含むネットワークを管理しています。管理者は、次世代ファイアウォールをルーテッドモードからトランスペアレントモードに変更する必要があります。この要件を満たすために、管理者は次にどのようなアクションを実行する必要がありますか？

- A. CLI からインターフェイス設定を手動で削除します。
- B. CLI から 1 つ以上のブリッジ グループを作成します。
- C. CLI から configure transparent firewall コマンドを入力します。
- D. Cisco Secure Firewall Management Center でファイアウォールの登録を解除します。

正解: ([正解を表示します](#))

質問: 112

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

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

正解: ([正解を表示します](#))

質問: 113

FlexConfigを使用せずにFirepower Threat Defenseでサポートされてい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. static routing
- D. IS-IS
- E. BGP

正解: B,E ([コメントを發表する](#))

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

質問: 114

クラスター化ユニット環境でサイト間VPNを設定することの欠点は何ですか？

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

正解: ([正解を表示します](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_g32_yml_y2b

質問: 115

ネットワーク管理者が、以前作成したファイルポリシーを新しいアクセスポリシーに適用しようとしています。ファイルポリシーを適用する前に、管理者はどのような操作を行う必要がありますか？

- A. アプリケーションをアクセス制御ルールに適用します。
- B. ファイルポリシーをデフォルトのアクションに割り当てます。
- C. 新しいアクセス制御ルールを作成します。
- D. 検査方針を策定する。

正解: ([正解を表示します](#))

質問: 116

エンジニアは、Cisco Firepower Management Centerで新しいIDポリシーを設定する必要があります。アクティブ認証は、Kerberos接続を使用して設定する必要があります。設定する必要がある2つのレルムはどれですか？

(2つ選択してください。)

- A. Active Directoryプライマリドメイン
- B. Active Directory参加ユーザー名
- C. ディレクトリユーザー名
- D. ディレクトリパスワード
- E. Active Directory参加パスワード

正解: ([正解を表示します](#))

質問: 117

エンジニアがCisco Secure Firewall Management CenterでCisco Secure Firewall Threat DefenseデバイスのURLフィルタリングを設定しています。ユーザーはアクセス時に警告を受け取る必要があります。

..www.badaduitsito.com にアクセスでき、必要に応じてウェブサイトを継続するオプションがあります。他のウェブサイトはブロックされません。これらの要件を無効にするには、エンジニアはどのような2つのアクションを実行する必要がありますか？

A. 設定

http://www.Dadadullsile.com の URL オブジェクトに一致するアクセス制御ルール

'そして、アクションをインタラクティブブロックに設定します。

B. アクセス制御ポリシーエディタの「HTTP レスポンス」タブで、「対話型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。

C. 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します。

D. 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ます。

E. 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。

正解: A,B ([コメントを发表する](#))

To

configure URL filtering such that users receive a warning when they access a specific website (e.g.,

http://www.badadultsite.com) and have the option to continue to the site, the engineer needs to perform the following actions:

Configure an access control rule:

Create

a URL object forhttp://www.badadultsite.com.

Set the action for this URL object to " Interactive Block, " which prompts the user with a warning and allows them to proceed if they choose to.

Set the Interactive Block Response Page:

Navigate to the HTTP Responses tab in the access control policy editor.

Set the Interactive Block Response Page to " System-provided " to ensure that users see the default warning page provided by Cisco Secure Firewall Management Center.

These actions ensure that only the specified website triggers an interactive block, while other websites are not blocked.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Access Control and URL Filtering.

質問: 118

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-reset
- 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-tuning

正解: **A** ([コメントを發表する](#))

質問: 119

エンジニアは、社内全体に展開されているさまざまなファイアウォールモデル(Cisco Secure Firewall Threat Defense、Cisco Secure firewall ASA、およびMeraki MXシリーズ)間で重複しているオブジェクトを特定するために、ネットワークプロジェクトの監査を実施するよう指示されました。この監査を実行する際に、エンジニアを支援するツールはどれですか？

- A. Cisco Firepower Device Manager
- B. Cisco SecureX
- C. Cisco Defense Orchestrator
- D. Cisco Secure Firewall Management Center

正解: ([正解を表示します](#))

Cisco Defense Orchestrator (CDO) is the tool that assists engineers in performing an audit of network projects to determine which objects are duplicated across various firewall models, including Cisco Secure Firewall Threat Defense, Cisco Secure Firewall ASA, and Meraki MX Series. CDO provides a unified management interface for managing multiple security devices and can identify duplicate objects across these devices.

Steps:

Access Cisco Defense Orchestrator.

Connect and synchronize all relevant firewall devices (FTD, ASA, Meraki MX).

Use the audit and reporting features in CDO to identify and manage duplicate objects.

This helps ensure consistency and efficient management across the organization ' s firewall deployments.

References: Cisco Defense Orchestrator Documentation, Chapter on Device Management and Object Auditing.

質問: 120

組織にはクライアントからサーバーを保護するためのコンプライアンス要件がありますが、クライアントとサーバーはすべて同じレイヤー3ネットワーク上にあります。クライアントまたはサーバーのIPサブネットを再アドレス指定せずに、セグメンテーションはどのように実現されますか？」

- A. クライアントとサーバーの間にファイアウォールを透過モードで展開します。
- B. 同じサブネットにとどまりながら、サーバーのIPアドレスを変更します
- C. 同じサブネット上にとどまりながら、クライアントのIPアドレスを変更します。

D. クライアントとサーバー間にルーティングモードでファイアウォールを展開します

正解: **A** ([コメントを发表する](#))

質問: **121**

管理者はCiscoASAからCiscoFTDアプライアンスへの移行に取り組んでおり、トラフィックを中断せずにルールをテストする必要があります。移行のこのフェーズでASAルールを設定するには、どのポリシータイプを使用する必要がありますか。

A. アイデンティティ

B. 侵入

C. アクセス制御

D. プレフィルター

正解: **C** ([コメントを发表する](#))

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

有効的な**300-710J**問題集はJPNTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-710J**試験問題集を提供します。JPNTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%**ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**

エンジニアが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 ツールに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を表示すると時間がかかり、目的のデータを見つけてフィルタリングするのが難しいことに気づきました。エンジニアは、この種の分析用に構築されたツールを使用してデータをレビューできるように、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

正解: ([正解を表示します](#))

When capturing traffic on a Cisco FTD device to troubleshoot a connectivity problem, a file type that can be exported for reviewing using a tool built for this type of analysis is PCAP. PCAP stands for Packet Capture and it is a file format used to store network packet data captured from a network interface⁸.

PCAP files contain the raw data of network packets, including the headers and payloads of each packet⁸.

PCAP files are widely used in network analysis and troubleshooting tasks. They enable network administrators, analysts, and researchers to inspect and analyze network traffic for various purposes, such as diagnosing network issues, detecting malicious activity, measuring network performance, and understanding network protocols⁸. PCAP files can be read by applications that understand that format, such as Wireshark, tcpdump, CA NetMaster, or Microsoft Network Monitor⁸.

The other options are incorrect because:

NetFlow v9 is not a file type, but a protocol for collecting and exporting information about network flows. A network flow is a sequence of packets that share common attributes such as source and destination IP addresses, ports, and protocols⁹. NetFlow v9 records contain summary information about network flows, such as start and end times, byte counts, packet counts, and so on⁹. NetFlow v9 records do not contain the raw data of network packets.

NetFlow v5 is not a file type, but an earlier version of the NetFlow protocol for collecting and exporting information about network flows. NetFlow v5 records contain similar information as NetFlow v9 records, but with fewer fields and less flexibility¹⁰. NetFlow v5 records do not contain the raw data of network packets.

IPFIX is not a file type, but a protocol for collecting and exporting information about network flows. IPFIX stands for IP Flow Information Export and it is based on NetFlow v9, but with some extensions and improvements¹¹. IPFIX records contain similar information as NetFlow v9 records, but with more fields and more flexibility¹¹. IPFIX records do not contain the raw data of network packets.

質問: 123

Cisco Secure Firewall Threat Defense 上の複数のインターフェイスを同じサブネット上に設定する機能はどれですか。

- A. すべて
- B. イーサチャネル
- C. セキュリティレベル
- D. BVI

正解: ([正解を表示します](#))

質問: 124

セキュリティアナリストは、Cisco FMC内に新しいレポートを作成して、毎日の攻撃、脆弱性、および接続の概要を示す必要があります。アナリストは、他のレポートの特定のダッシュボードを再利用して、この統合されたダッシュボードを作成したいと考えています。このタスクを実行するアクションはどれですか？

- A. Cisco FMC内のカスタムワークフローを変更して、目的のデータを新しいレポートにフィードします。
- B. 目的のビューを表すために、オブジェクト管理を介して新しいダッシュボードオブジェクトを作成します。
- C. 新しく作成されたレポートのインポート機能を使用して、追加するダッシュボードを選択します。
- D. マルウェアレポートをコピーし、セクションを変更して、他のレポートからコンポーネントをプルします。

正解: ([正解を表示します](#))

質問: 125

ネットワークエンジニアがCiscoAMP for Endpointsコンソールにログインし、識別されたSHA-256ハッシュに対する悪意のある判定を確認します。この脅威を軽減するには、どの構成が必要ですか？

- A. 感染したエンドポイント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. ハッシュを単純なカスタム削除リストに追加します。
- C. 正規表現を使用して悪意のあるファイルをブロックします。
- D. 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。

正解: ([正解を表示します](#))

質問: 126

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

- A. デバイスごとに一意のACPを作成する
- B. CiscoTalosから更新される動的ACPを利用する
- C. ポリシーの継承を利用する
- D. 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

正解: ([正解を表示します](#))

質問: 127

CEOはネットワーク管理者に、上位のDNSクエリ、URLカテゴリ統計、およびURL評判統計に関する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た。

管理者は、経営陣にこの情報を迅速に提供するために、どのような行動を取るべきでしょうか？

- A. 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。
- B. 攻撃レポートを実行し、DNSでフィルタリングしてこの情報を表示します。
- C. 侵入イベントダッシュボードタブをコピーし、各ウィジェットを修正して正しいグラフを表示するようにします。
- D. 接続イベントダッシュボードを変更して、管理用のビューで情報を表示するようにします。

正解: A ([コメントを發表する](#))

質問: 128

管理者は、ネットワークパフォーマンスを向上させるためにCisco FTDルールを最適化しており、Cisco FTDへの負荷を軽減するために特定のトラフィックタイプの検査をバイパスしたいと考えています。この目的を達成するには、どのポリシーを設定する必要がありますか？

- A. アイデンティティ
- B. プリフィルタ
- C. URLフィルタリング
- D. 侵入

正解: ([正解を表示します](#))

質問: 129

インターフェイスにヒットするすべてのパケットをキャプチャするには、Cisco FTD CLIでどのコマンドを使用する必要がありますか？

- A. コアダンプパケットエンジンを有効にする
- B. キャプチャトラフィック
- C. キャプチャ
- D. WORDをキャプチャする

正解: ([正解を表示します](#))

Reason: the command " capture-traffic " is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the " capture " command. Since the Lina Engine represents the actual physical interface of the device, " capture " is the only reasonable choice

Reference:<https://www.cisco.com/c/en/us/support/docs>

/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10 The command is firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

質問: 130

ネットワーク管理者が新しい Cisco Secure Firewall Threat Defense (FTD) ファイアウォールを導入しています。Cisco Secure FTD の導入後、内部クライアント間の接続が断続的になります。Secure FTD ファイアウォールでパケットキャプチャを実行すると、Secure FTD 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がわかります。ネットワーク管理者は、この問題を解決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. NATポリシーを確認し、不適切なプロキシARP設定を無効にします。
- 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. ARP リクエストを許可するために FTD を透過モードに変換します。

正解: A ([コメントを发表する](#))

If inside clients have intermittent connectivity issues and the Cisco Secure FTD is responding to all ARP requests on the inside network, it indicates that there may be an incorrect proxy ARP configuration in the NAT policy. Proxy ARP can cause the FTD to respond to ARP requests on behalf of other devices, leading to connectivity issues.

Steps to resolve:

Review the NAT policy on the FTD to identify any incorrect proxy ARP configurations.

Disable the proxy ARP setting for the relevant NAT rules that are causing the issue.

This ensures that the FTD only responds to ARP requests as needed, preventing it from interfering with normal ARP traffic on the inside network.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on NAT and ARP Configuration.

質問: 131

2つのCisco FTDデバイス間で高可用性が機能するために必要な2つの条件はどれですか。

(2つ選択してください。)

- A. ユニットは同じバージョンである必要があります
- B. 両方のデバイスは、FMC内で構成されている場合、同じドメインにある必要がある別のグループの一部になることができます。
- C. ユニットが同じシリーズの一部である場合、ユニットは異なるモデルでなければなりません。
- D. ユニットは、ファイアウォールルーテッドモードでのみ構成する必要があります。
- E. ユニットは同じモデルでなければなりません。

正解: A,E ([コメントを发表する](#))

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-fire.html>

質問: 132

Cisco Threat Response によるインシデント調査を簡素化するコンポーネントはどれですか？

- A. Cisco AMP クライアント
- B. ローカル CVE データベース
- C. Cisco Secure Firewall アプライアンス
- D. ブラウザプラグイン

正解: ([正解を表示します](#))

Cisco Threat Response (CTR) is a security solution that helps simplify incident investigation and threat hunting. One of its components that significantly simplifies the investigation process is the browser plug-in.

The browser plug-in integrates with CTR to provide contextual information directly within the browser, allowing security analysts to quickly view threat details, pivot to related information, and take appropriate actions without switching between multiple tools.

Features of the browser plug-in:

- * Provides real-time threat intelligence and context from various Cisco security products.
- * Allows security analysts to investigate incidents directly from web-based consoles.
- * Enhances efficiency by streamlining the workflow and reducing the time needed to gather and correlate information.

References: Cisco Threat Response Documentation, Browser Plug-in Section.

質問: 133

管理者は、インライン IPS 展開で Cisco Secure Firewall Threat Defence デバイスのインターフェイスを設定します。管理者は次のアクションを実行します。

- * デバイスとインターフェイスを識別します
- * インターフェイ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どれですか？

- 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.** インターフェイ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。

正解: ([正解を表示します](#))

After setting the interface mode to inline and enabling the interfaces on a Cisco Secure Firewall Threat Defense (FTD) device in an inline IPS deployment, the next step is to configure an inline set. An inline set groups two interfaces that work together to inspect traffic passing between them.

Steps to configure an inline set:

In FMC, navigate to Devices > Device Management.

Select the FTD device and configure the interfaces.

Create a new inline set, adding the relevant interfaces that have been set to inline mode.

Deploy the configuration to the FTD device.

Configuring an inline set ensures that the traffic between the specified interfaces is inspected and processed according to the IPS policies, completing the implementation of the inline IPS deployment.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Inline Sets.

質問: 134



図を参照してください。エンジニアが、インターフェースをIPSインラインペアモードにしてCisco Secure Firewall Threat Defenseのインスタンスを設定しています。要件を満たすために、インターフェースe1/6には何を設定する必要がありますか？

- A. リンク状態の伝播が無効になっています
- B. セキュリティゾーンをOUTSIDE_ZONEに設定
- C. インラインセットMTUを1500に設定
- D. フェイルセーフ無効

正解: ([正解を表示します](#))

質問: 135

エンジニアは、Cisco FTD デバイスでリモート アクセス VPN をセットアップしており、VPN トンネル経由で送信されるトラフィックを定義したいと考えています。このタスクを実行するには、Cisco FMC でどの名前付きオブジェクト タイプを使用する必要がありますか？

- A. 路線図
- B. アクセスリスト
- C. クリプト マップ
- D. スプリット トンネル

正解: ([正解を表示します](#))

質問: 136

管理者は、QoS ポリシーを Cisco FTD 展開に追加しています。新しいルールがポリシーに追加され、QoS が 宛先インターフェース オブジェクト内の「インターフェース」に適用されると、使用可能なインターフェース オブジェクトがありません。問題は何ですか？

- A. 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
- B. インターフェイスが存在するネットワーク セグメントには、連続した IP 空間がありません。
- C. QoS はルーテッド インターフェイスでのみ使用でき、このデバイスはトランスペアレント モードです。
- D. QoS の追加を妨げている宛先インターフェース タイプ間に競合が存在します。

正解: C ([コメントを发表する](#))

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **137**

Cisco Firepower Management Center CLIでサポートされているコマンドラインモードはどれですか。

- A. 特権
- B. ユーザー
- C. 構成
- D. 管理者

正解: **C** ([コメントを发表する](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command_line_reference.pdf

質問: **138**

セキュリティエンジニアは、Cisco Secure Firewall Threat Defenseデバイス上に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。

ソリューションでは、PDF、DOCX、および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設定する必要があることは何ですか？

- 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

正解: ([正解を表示します](#))

To create a malware and file policy on a Cisco Secure Firewall Threat Defense (FTD) device that ensures PDF, DOCX, and XLSX files are not sent to Cisco Secure Malware Analytics, the security engineer must configure local malware analysis. Local malware analysis allows the FTD to inspect and analyze files locally without sending them to the cloud-based Cisco Secure Malware Analytics.

Steps to configure local malware analysis:

In FMC, navigate to Policies > Access Control > Malware & File Policies.

Create a new malware and file policy or edit an existing one.

Define rules to inspect specific file types, ensuring that PDF, DOCX, and XLSX files are handled locally.

Set the action for these file types to "Local Analysis."

Apply the policy to the relevant access control policy.

This configuration ensures that the specified file types are analyzed locally, meeting the requirement to avoid sending them to Cisco Secure Malware Analytics.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Malware and File Policies

質問: **139**

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

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

正解: ([正解を表示します](#))

Reference:

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

質問: 140

セキュリティ エンジニアは、1 つのサーバーへの UDP トラフィックをブロックする新しいポリシーを追加する必要があります。エンジニアは新しいオブジェクトを追加します。すべての UDP ポートを識別するために、エンジニアは次にどの操作を行う必要がありますか？

- A. UDP と TCP に対応する IP プロトコル番号を追加します。
- B. トランスポート プロトコルを指定し、ポート番号を空にします。
- C. トランスポート番号を追加し、タイプとコードを指定します。
- D. トランスポート プロトコルと必須のポート範囲を定義します。

正解: ([正解を表示します](#))

質問: 141

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

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

正解: ([正解を表示します](#))

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower-management-center-display-acc.html>

質問: 142

エンジニアが、現在のファイアウォールを置き換えるために、新しい Cisco Secure Firewall Threat Defense アプライアンスをセットアップしています。会社は、インライン セットを使用し、インライン セットの 1 つのインターフェイスがダウンすると、インライン セットの 2 番目のインターフェイスもダウンするように要求しています。展開要件を満たすために、エンジニアは何を構成する必要がありますか？

- A. リンク ステートの伝播
- B. インライン タップ モード
- C. Snort フェイル オープン
- D. 厳密な TCP 強制

正解: ([正解を表示します](#))

質問: 143

2つのアプリケーション層プリプロセッサとは何ですか？ 2つ選択してください。）

- A. CIFS

- B. IMAP
- C. SSL
- D. DNP3
- E. ICMP

正解: ([正解を表示します](#))

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

質問: 144

しきい値設定を構成できる2つの場所はどれですか。 2つ選択してください。)

- A. 各IPSルール
- B. グローバルに、ネットワーク分析ポリシー内
- 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について
- E. プリプロセッサごと、ネットワーク分析ポリシー内

正解: ([正解を表示します](#))

Reference: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-Threshold.pdf>

質問: 145

Cisco Secure Firewall Management CenterをpxGridと統合するために、Cisco ISEからエクスポートする必要がある証明書の種類はどれですか？

- A. ドメインコントローラーからの自己署名SAML証明書
- B. pxGridサーバーノードの認証局証明書
- C. 第三者によって署名された自己署名認証局証明書
- D. ドメインの公開鍵証明書

正解: ([正解を表示します](#))

Secure Firewall Management Center must trust the certificate presented by the Cisco ISE pxGrid server.

Therefore, the certificate authority certificate that signed the pxGrid node's server certificate must be exported from ISE and imported into Management Center as a trusted CA object. If primary and secondary pxGrid nodes are deployed, Cisco requires their certificates to be signed by the same trusted certificate authority.

Depending on the integration design, the engineer might also need the monitoring-node CA certificate and a pxGrid client certificate with its private key for Management Center. However, the question specifically asks which certificate establishes trust with the pxGrid server node. SAML and domain-controller certificates are unrelated, and a certificate cannot simultaneously be self-signed and signed by a third-party CA. Cisco ISE and Secure Firewall certificate integration

質問: 146

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

- A. マルウェアクラウドルックアップと動的分析
- B. マルウェアのアクションと動的分析をブロックする
- C. マルウェアアクションとローカルマルウェア分析をブロックする

D. ブロックファイルアクションとローカルマルウェア分析

正解: ([正解を表示します](#))

質問: 147

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

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

正解: ([正解を表示します](#))

質問: 148

エンジニアは、Cisco Secure Firewall Management Center バージョン 7.0 で URL フィルタリングを展開する必要があります。エンジニアは、不正な動作を示す、または悪意のある、あるいは望ましくない Web サイトをフィルタリングするためのアクセス制御ルールの URL 条件を設定しています。どのレピュテーションレベルを設定する必要がありますか？

- A. 疑わしい**
- B. 信頼できない**
- C. 好ましい**
- D. ニュートラル**

正解: ([正解を表示します](#))

The Untrusted reputation level represents URLs associated with malicious, undesirable, or demonstrably unsafe behavior and is therefore the appropriate selection for the access control rule. Questionable applies to URLs that exhibit suspicious characteristics but lack sufficient evidence to be classified as definitively malicious. Neutral identifies sites without a strong positive or negative reputation, while Favorable indicates generally acceptable sites with a positive reputation history. Secure Firewall Management Center combines URL categories with reputation values to provide more precise web-control decisions. Selecting Untrusted enables the rule to match the highest-risk URLs covered by the requirement without unnecessarily treating merely unknown or neutral sites as confirmed threats. Cisco documents URL reputation as the risk component used with URL categories in category-and-reputation-based filtering. Cisco Secure Firewall URL filtering

質問: 149

エンジニアは、Cisco Secure Firewall Management Centerを使用す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、各ネットワークの該当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で設定する必要がある項目は何ですか？

- A. 上書きを許可するチェックボックス**
- B. IP範囲**
- C. ICMP拒否チェックボックス**
- D. IPアドレス**

正解: ([正解を表示します](#))

質問: 150

エンジニアが Cisco FMC でカスタム侵入ルールを設定しています。エンジニアは、ペイロードまたはストリームから文字列 " |45 5* 26 27 4 0A|* " を検索するルールが必要です。パックされた検査の引数を作成するために、エンジニアはこの文字列とともにどのキーワードを使用する必要がありますか？

- A. メタデータ
- B. 内容
- C. 保護されたコンテンツ
- D. データ

正解: ([正解を表示します](#))

The content keyword is used to specify a string or pattern to search for in the payload or stream of a packet.

The string must be enclosed in quotation marks and can use modifiers such as nocase, depth, offset, and so on.

The string can also use hexadecimal notation by using a pipe symbol (|) before and after the hexadecimal characters. For example, content: " |45 5* 26 27 4 0A| " will match any payload or stream that contains the hexadecimal bytes 45 5 26 27 4 0A followed by any number of bytes2

質問: 151

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

- A. Cisco FMC内のAPI制限により、ウィジェットが表示されません。
- 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. ウィジェットは、アクティブなイベントが存在する場合にのみ表示されるように設定されています。
- D. ウィジェットは Cisco FMC 内で設定されていません。

正解: ([正解を表示します](#))

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**3 0 %ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 152

エンジニアは、アプリケーションの使用状況を毎月自動的に表示し、その情報を管理者に送信するように求められました。このタスクを実行するには、どのメカニズムを使用する必要がありますか？

- A. reports
- B. context explorer
- C. event viewer
- D. dashboards

正解: ([正解を表示します](#))

質問: 153

Cisco FMCを介してデバイスを管理しながらデバイスを削除および再追加する場合、どの2つの考慮事項を考慮する必要がありますか 2つ選択してください)。

- A. 登録時にNATおよびVPNポリシーを再適用するオプションが利用可能であるため、ユーザーは登録の完了後にポリシーを再適用する必要はありません。

- B. Cisco FMC Webインターフェイスは、アクセス制御ポリシーを再適用するようにユーザに要求します。
- C. デバイスを再度追加する前にCisco FMCでは、マネージャを再度追加する必要があります。
- D. 登録時にNATおよびVPNポリシーを再適用するオプションはありません。そのため、ユーザーは登録の完了後にポリシーを再適用する必要があります。
- E. デバイスが削除されたら、CiscoFMCに再追加する前に再設定する必要があります。

正解: B,D ([コメントを發表する](#))

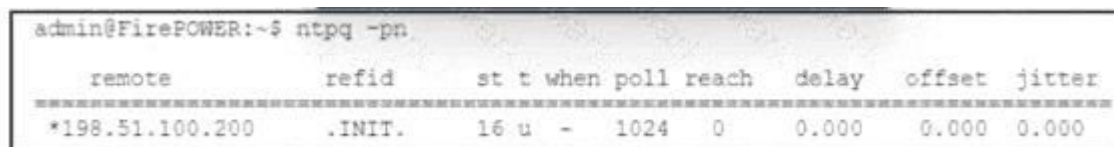
質問: 154

Cisco AMP for Endpointsの2つの機能で、アップロードされたファイルをブロックできますか？ 2つ選択してください。）

- A. アプリケーションのブロック
- B. 簡単なカスタム検出
- C. ファイルリポジトリ
- D. アプリケーションのホワイトリスト
- E. 除外

正解: A,B ([コメントを發表する](#))

質問: 155



remote	refid	st	t	when	poll	reach	delay	offset	jitter
*198.51.100.200	.INIT.	16	u	-	1024	0	0.000	0.000	0.000

図を参照してください。セキュリティ エンジニアは、Web インターフェイスのヘルス モニタを使用して、Cisco Secure Firewall Management Center でヘルス アラートを表示します。アラートの 1 つで、時刻同期モジュールの状態が同期していないため、アプライアンスがクリティカルであると表示されます。問題をトラブルシューティングするために、エンジニアは Secure Firewall Management Center で ntpq コマンドを実行します。出力は図に示されています。セキュリティ エンジニアは、この問題を解決するために次にどの操作を行う必要がありますか？

- A. タイム サーバーへの接続を再確立します。
- B. アプライアンスが自身の内部時計と同期するように設定します。
- C. アプライアンスが NTP サーバーから時刻を受信するように設定します。
- D. アプライアンスをハード リブートしてリセットします。

正解: ([正解を表示します](#))

質問: 156

Cisco FMCのポートオブジェクトの機能は何ですか。

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

正解: B ([コメントを發表する](#))

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

質問: 157

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。エンジニアはどの2つの操作を行う必要がありますか？(2つ選択してください。)

- A. セキュリティインテリジェンスオブジェクトを設定して、データをCisco Secure Network Analyticsに送信するようにします。
- B. Netflow_Send_Destination オブジェクトを構成に追加します。
- C. NetFlowサービスを有効にするためのサービス識別子を作成します。
- D. Netflow_Set_Parameters オブジェクトを構成に追加します。
- E. Netflow_Add_Destination オブジェクトを構成に追加します。

正解: (正解を表示します)

質問: 158

どのオブジェクトタイプがオブジェクトのオーバーライドをサポートしていますか？

- A. 時間範囲
- B. セキュリティグループタグ
- C. ネットワークオブジェクト
- D. DNSサーバーグループ

正解: (正解を表示します)

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

質問: 159



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)
BitTorrent	0	Very High	Very Low	1.7281
TOR	5	Medium	Low	0.0006
SSL client	10,100	Medium	Medium	48.4102
Skype	644	Medium	Medium	10.3545
cURL	280	Medium	Medium	0.4840

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。不正なネットワーク使用を防ぐために、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. YouTube
- C. クローム
- D. TOR

正解: D (コメントを發表する)

質問: 160

FTDでトラブルシューティングファイルを生成するには、どのコマンドを実行する必要がありますか？

- A. システムサポートビューファイル
- B. sudo sf_troubleshoot.pl
- C. システムはすべてトラブルシューティングを生成します

D. 技術サポートを表示する

正解: ([正解を表示します](#))

Reference: <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote- SourceFire-00.html>

質問: 161

Cisco Secure Firewall デバイスに統合ルーティングおよびブリッジング (IRB) を実装するメリットは何ですか？

- A. デバイス上の複数の物理インターフェースを同じVLAN上に配置できます。
- B. デバイスが単一障害点となることを防ぐことで、稼働時間が向上します。
- C. セキュリティポリシーが異なる顧客が同じデバイスに存在できます。
- D. 脅威情報はCisco Talosから動的に更新されます。

正解: **A** ([コメントを發表する](#))

Integrated Routing and Bridging allows a Secure Firewall device operating in routed mode to contain bridge groups while also supporting routed interfaces. Multiple physical or logical interfaces can become members of one bridge group, placing them in the same Layer 2 broadcast domain, VLAN, and IP subnet. A Bridge Virtual Interface represents that bridge group at Layer 3 and functions as its gateway, permitting communication between the bridged network and routed interfaces or other bridge groups, subject to security policy. This can remove the need for an additional external Layer 2 switch when suitable firewall interfaces are available. IRB does not itself provide high availability, security-context separation, or Cisco Talos threat- intelligence updates. Those capabilities are implemented through separate features. Therefore, allowing multiple interfaces to participate in the same VLAN is the stated IRB benefit. Cisco IRB documentation

質問: 162

非同期ルーティング構成を展開するときに、同じインラインインターフェイスセットに複数のインラインインターフェイスペアを追加する利点は何ですか？

- A. IPSがインバウンドトラフィックとアウトバウンドトラフィックを同じトラフィックフローの一部として識別できるようにします。
- B. インターフェースは自動ネゴシエーションを無効にし、インターフェース速度はハードコードされて1000Mbpsに設定されます。
- C. Snortプロセスの再起動中に、トラフィック検査を中断することなく続行できます。
- D. インターフェースは、メディアに依存しないインターフェイスクロスオーバーとして自動的に構成されます。

正解: **A** ([コメントを發表する](#))

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v601_chapter_01011010.pdf

質問: 163

ネットワークエンジニアが、Cisco Secure Firewall Management CenterとCisco Secure Firewall Threat Defense間の接続問題を検出しました。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、エンジニアはどの2つのコマンドを実行する必要がありますか？(2つ選択してください。)

- A. 履歴を表示
- B. `sudo perfstats -Cq < /var/sf/rna/correlator-stats/now`
- C. `sudo stats_unified.pl`
- D. ディスクマネージャを表示する
- E. `manage_procs.pl`

正解: ([正解を表示します](#))

質問: 164

エンジニアが Cisco FMC で URL オブジェクトを作成しています。オブジェクトがアクセス コントロール ポリシーの HTTPS トラフィックと一致するようになるには、どのように設定する必要がありますか？

- A. Web サイト証明書のサブジェクト共通名を使用します
- B. HTTPS を使用する個々の Web ページへのパスを定義します。
- C. Web サイトのサブドメインを含む FQDN を使用します。
- D. 一致させるプロトコル (HTTP または HTTPS) を指定します。

正解: ([正解を表示します](#))

質問: 165

エンジニアは Cisco FTD デバイスを導入する必要があります。管理者は、エンド ユーザーに混乱をもたらすネットワーク変更を必要とせずにトラフィックを調査したいと考えています。企業のセキュリティ ポリシーでは、管理トラフィックをデータ トラフィックから分離し、リモート管理に Telnet 経由の SSH を使用することが必要です。これらの要件を満たすには、デバイスをどのように展開する必要がありますか？

- A. 診断インターフェイスを使用したルーテッド モード
- B. 管理インターフェイスを使用した透過モード
- C. データインターフェイスで作成された透明な
- D. ブリッジ仮想インターフェイスを使用したルーテッド モード

正解: B ([コメントを發表する](#))

To deploy a Cisco FTD device that meets the requirements of the question, the engineer must use transparent mode with a management interface. Transparent mode is a firewall configuration in which the FTD device acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the FTD device can examine traffic without requiring network changes that will disrupt end users, such as changing IP addresses or routing configurations¹. A management interface is a dedicated interface that is used for managing the FTD device and separating management traffic from data traffic. A management interface can be configured to allow SSH access for remote administration, which is more secure than Telnet².

The other options are incorrect because:

- * Routed mode is a firewall configuration in which the FTD device acts as a router and performs address translation and routing for connected networks. Routed mode requires network changes that may disrupt end users, such as changing IP addresses or routing configurations¹. A diagnostic interface is a special interface that is used for troubleshooting and capturing traffic on the FTD device. A diagnostic interface does not separate management traffic from data traffic or allow SSH access for remote administration.
- * Transparent mode with a data interface does not meet the requirement of separating management traffic from data traffic. A data interface is a regular interface that is used for passing and inspecting traffic on the FTD device. A data interface does not allow SSH access for remote administration².
- * Routed mode with a bridge virtual interface (BVI) does not meet the requirement of examining traffic without requiring network changes that will disrupt end users. A BVI is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. A BVI allows the FTD device to route between different bridge groups on the same security module/engine. However, routed mode still requires network changes that may disrupt end users, such as changing IP addresses or routing configurations.

質問: 166

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

- A. パフォーマンスを向上させるために複数のCisco FTDHAペアを導入する
- B. パフォーマンスを向上させるために、ファイアウォールクラスタリングモードで複数のCiscoFTDアプライアンスを導入します。
- C. パフォーマンスを向上させるためにクラスタリングモードで複数のCisco FTDHAペアを導入する
- D. 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。

正解: **B** ([コメントを发表する](#))

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **167**

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ようにCiscoFTD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、CiscoCatalyst9300スイッチからミラーリングされます。どの構成がタスクを実行しますか？

- A. インターフェース構成モードをnoneに設定します。
- B. インターフェース構成モードをパッシブに設定します。
- C. ファイアウォールモードを透過に設定します。
- D. ファイアウォールモードをルーティングに設定します。

正解: ([正解を表示します](#))

質問: **168**

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

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

正解: ([正解を表示します](#))

質問: **169**

インターフェイスの最大スループットより大きいレート制限を持つQoSルールを指定した結果はどうなりますか？

- A. レート制限ルールは無効になっています。
- B. 一致するトラフィックはレート制限されません。
- C. システムはすべてのトラフィックをレート制限します。
- D. システムは繰り返し警告を生成します。

正解: ([正解を表示します](#))

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

質問: 170

エンジニアは、マルチドメイン展開で Cisco FMC ダッシュボードを設定する必要があります 先祖ドメインからレポート テンプレートを編集するためにエンジニアが実行する必要があるアクションはどれですか？

- A. 現在のドメインにコピーします
- B. 別のウィジェットとして追加します。
- C. 自分自身に所有権を割り当てます
- D. ドキュメントの属性を変更します。

正解: ([正解を表示します](#))

質問: 171

Cisco Threat Responseでの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. ブラウザ拡張機能を介してデータをプルする
- C. アラート付きのトリアージオートマトン
- D. アラートの優先順位付け

正解: A ([コメントを發表する](#))

The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.

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

質問: 172

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

- A. プレフィルタポリシーを使用してVPNトラフィックを無視するようにCiscoFirepowerデバイスを設定します
- B. flexconfigポリシーを有効にして、VPNトラフィックを再分類し、対象のトラフィックとして表示されないようにします。
- C. VPNトラフィックのアクセス制御ポリシーをバイパスするようにCiscoFirepowerデバイスを設定します。
- D. VPNトラフィックが検査なしで通過できるように、侵入ポリシーを調整します

正解: C ([コメントを發表する](#))

When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

Reference:<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-cisco-firepow.html>

質問: 173

複数のドメインが使用されているマルチテナント環境において、グローバルドメインの外側に適用すべきアップデートはどれですか？

- A. 侵入ルールのローカルインポート
- B. 主要アップグレードの現地輸入

C. シスコ位置情報データベース

D. マイナーアップグレード

正解: ([正解を表示します](#))

質問: 174

ネットワークエンジニアは、2つのCiscoFTD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、および接続の更新が含まれている必要があります。2つのアプライアンスの初期構成後、冗長構成を続行するには、どの2つの手順を実行する必要がありますか？ 2つ選択してください。)

A. フェイルオーバーリンクで仮想MACアドレスを構成します。

B. スタンバイIPアドレスを設定します。

C. ステートフルプロパティを使用してフェイルオーバーリンクを構成します。

D. 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。

E. 内部インターフェイスでhelloを無効にします。

正解: ([正解を表示します](#))

質問: 175

ある企業が、Cisco FMCで管理されるCisco FTDを使用して侵入防止システムを導入する過程にある。

エンジニアは、潜在的な侵入を検知しつつ、疑わしいトラフィックをブロックしないようにポリシーを設定する必要があります。このタスクを達成するには、どの操作を実行すればよいでしょうか？

A. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプションのチェックを外して IPS モードを設定します。

B. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプション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際に、「インライン時にドロップ」オプションをオンにして、IDS モードを設定します。

D. アクセス ポリシー セクションの Cisco FMC 侵入タブでポリシー ルールを作成または編集する際に、「インライン時にドロップ」オプションをオンにして、IPS モードを設定します。

正解: ([正解を表示します](#))

質問: 176

ある企業は、CiscoFMCによって管理されているCiscoFTDを使用して侵入防御を展開しているところです。より少ないルールで重大な状態のみを検出し、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. バランスの取れたセキュリティと接続性

B. アクティブなルールはありません

C. 最大検出

D. セキュリティを介した接続

正解: ([正解を表示します](#))

質問: 177

ネットワーク管理者は、CIOの月次セキュリティレポートの作成中に見られた疑わしいMicrosoft実行可能ファイルの種類に関する懸念から、マルウェア検出による機械学習を有効にすることで、ネットワークセキュリティ体制を強化したいと考えています。この目標を達成するには、どの機能を有効にする必要がありますか？

- A. 静的分析
- B. スペロ
- C. 動的解析
- D. エートス

正解: ([正解を表示します](#))

質問: 178

エンジニアは、Cisco Secure Firewall Management Center (FMC) インベントリ内の Cisco Secure Firewall Threat Defense (FTD) ファイアウォールのモードを変更する必要があります。エンジニアは次のアクションを実行する必要があります。

- * Secure FTD を Secure FMC に登録します。
- * ファイアウォールモードを変更します。
- * Secure FMC から Secure FTD デバイスの登録を解除します。

エンジニアは FTD に対してどのようなアクションを取る必要がありますか？

- A. Secure FTD デバイスをリロードします。
- B. 管理 IP アドレスを設定します。
- C. コンソール ポートから Secure FTD CLI にアクセスします。
- D. Secure FTD 設定を消去します

正解: ([正解を表示します](#))

To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps:

Register the Secure FTD with Secure FMC.

Change the firewall mode.

Deregister the Secure FTD device from Secure FMC.

To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and manage the registration status of the FTD device.

Steps:

Connect to the Secure FTD device via the console port.

Access the CLI and execute the command to change the firewall mode (configure firewall-mode).

Deregister the device from FMC if needed.

Register or re-register the device with FMC as required.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Device Management and CLI Access.

質問: 179

Cisco Firepower Threat Defenseで有効なルーティングオプションはどれですか？ 2つ選択してください。）

- A. BGPv6
- B. 複数のインターフェイス間で最大3つの等コストパスを備えたECMP
- C. 単一インターフェイス全体で最大3つの等コストパスを備えたECMP

- D. トランスペアレントファイアウォールモードのBGPv4
- E. ノンストップフォワーディングを使用するBGPv4

正解: **A,C** ([コメントを发表する](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

質問: **180**

組織は、新しい Cisco FTD アプライアンスをネットワークに設置しています。エンジニアは、同じ 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構成する任務を負っています。このタスクを達成するために必要な手順はどれですか？

- 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. 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。
- D. ループを防ぐために BPDU パケットを許可します。

正解: ([正解を表示します](#))

質問: **181**

エンジニアが、ネットワークを保護するために Cisco IPS を構成しており、展開する前にポリシーをテストしたいと考えています。トラフィック フローが一定の間である間、受信パケットのコピーを監視する必要があります。これらの要件を満たすために実装する必要がある IPS モードはどれですか？

- A. パッシブ
- B. トランスペアレント
- C. ルーテッド
- D. インライン タップ

正解: **D** ([コメントを发表する](#))

有効的な**300-710J**問題集はJPNTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-710J**試験問題集を提供します。JPNTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **182**

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. レイヤー7ネットワークID
- B. ソースIP
- C. アプリケーションID
- D. 動的なファイアウォールのインポート
- E. プロトコル

正解: ([正解を表示します](#))

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

質問: 183

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

A. 利用できません

B. 不明

B. きれい

C. 切断された

正解: ([正解を表示します](#))

質問: 184

エンジニアは、内部ネットワークの IP アドレスが既知の悪意のあるホストと通信しているかどうかを検出するために、Cisco Secure Firewall Management Center で関連ポリシーを構成する必要があります。内部 IP アドレスによって行われた接続を追跡し、条件には外部の動的リストを使用する必要があります。エンジニアは、関連ポリシーでどのタイプのイベントを構成する必要がありますか？

A. ネットワーク検出

B. 接続トラッカー

C. マルウェア

D. 侵入影響アラート

正解: B ([コメントを发表する](#))

質問: 185

ネットワーク管理者が既存のFMCに新しいFTDを登録しました。管理者はFTDを透過モードに設定できません。透過モードを有効にするには、どの操作を実行すればよいでしょうか？

A. 2つの物理インターフェースにIPアドレスを割り当てます。

B. 透過モードを設定する前に、FTD にブリッジ グループ インターフェイスを追加してください。

C. FMCからFTDデバイスの登録を解除し、CLI経由で透過モードを設定します。

D. 透過モードをサポートするFTDモデルを取得します。

正解: ([正解を表示します](#))

質問: 186

最近の夏時間の変更により、システムログには、リアルタイムより1時間遅れて発生したアクティビティが表示されます。この問題を解決するには、どのアクションを実行する必要がありますか？

A. すべての管理対象デバイスで時間を手動で正しい時間に調整します

B. NTPを使用するようにシステムクロック設定を構成します

C. 夏時間をチェックしてNTPを使用するようにシステム時刻設定を構成します

D. CiscoFMCで時間を手動で正しい時間に調整します。

正解: ([正解を表示します](#))

質問: 187

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

- A. リードドメイン
- B. セカンドレベルドメイン
- C. グローバルドメイン
- D. サブドメイン

正解: **A** ([コメントを发表する](#))

質問: 188

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

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

正解: ([正解を表示します](#))

質問: 189

展示資料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モードでインラインセットと共に展開されています。ネットワークエンジニアは、ルーティングされたルーター R1 と Secure FTD デバイス間のケーブルが切断されたときに、ルーター R2 が直接接続されているルート M 68.1.0/24 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？

1

- A. セキュアFTDデバイスで「リンクの劣化を伝播する」オプションを実装する
- B. R1とR2の間でルーティングプロトコルを確立します。
- C. セキュアFTDデバイスのハードウェアバイパスを無効にします。
- D. R2のGi0/2インターフェイスに自動状態機能を実装する

正解: ([正解を表示します](#))

To ensure that router R2 removes the directly connected route for 192.168.1.0/24 from its routing table when the cable between router R1 and the Secure FTD device is disconnected, the network engineer must implement the " Propagate Link State " option on the Secure FTD device. This option allows the FTD to propagate the link state changes to adjacent devices, ensuring that the disconnection is recognized and the routing table is updated accordingly.

Steps:

Access the FTD device configuration via FMC.

Navigate to the interface settings for the relevant interfaces.

Enable the " Propagate Link State " option for the interfaces connected to R1 and R2.

Deploy the changes to the FTD device.

This configuration ensures that the link state changes are communicated to router R2, prompting it to remove the disconnected route from its routing table.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Interface Settings and Link State Propagation.

質問: 190

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、どの通信がブロックされますか？

- A. インターネットで
- B. お互いに
- C. 他のルーターを使用する場合
- D. クライアントデバイスを使用する場合

正解: ([正解を表示します](#))

質問: 191

展示資料を参照してください。

このウェブサイトへのアクセスを修復しつつ、他のすべてのウェブサイトへの同様の通信を防止するには、どのような対策を講じるべきでしょうか？

- A. ポート443を172.1.1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。50
- B. 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。
- C. Snortがポート443を172.1.1.50のみに許可するようにする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。

正解: ([正解を表示します](#))

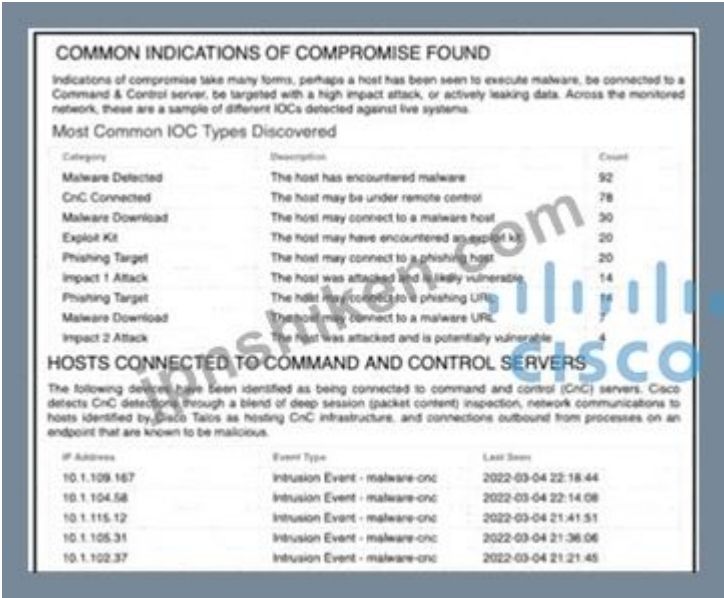
質問: 192

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

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

正解: ([正解を表示します](#))

質問: 193



図を参照してください。エンジニアがCisco Secure Firewall Management Centerのネットワークリスクレポートを分析しています。このリスクを軽減するために、エンジニアはどのような対策を推奨すべきでしょうか？

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

正解: B ([コメントを发表する](#))

質問: 194

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が使用されます。高可用性ピアの両方で、それぞれ独立して選択する必要がある設定はどれですか？(2つ選択してください。)

- A. セキュアエンドポイントクラウド接続
- B. スマートソフトウェアマネージャサテライト
- C. インターネット接続
- D. シスコサクセスネットワーク
- E. セキュリティグループタグ

正解: A,C ([コメントを发表する](#))

質問: 195

ネットワークエンジニアは、トラフィックを検査してIDSとして機能するように、Cisco Secureファイアウォール脅威防御デバイスでIPSモードを設定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脅威防御デバイスのパッシブインターフェイスとスイッチのSPANを設定済みです。次にエンジニアが設定する必要があるのは何ですか？

- A. セキュアファイアウォール脅威防御デバイスにおける侵入ポリシー
- B. 私のセキュアファイアウォール脅威防御デバイス上のアクティブなインターフェース
- C. スwitchのDHCP
- D. スwitch上のアクティブなSPANポート

正解: ([正解を表示します](#))

To configure IPS mode on a Cisco Secure Firewall Threat Defense (FTD) device to inspect traffic and act as an IDS, the network engineer must configure an intrusion policy on the FTD device. The passive-interface and SPAN on the switch have already been configured, which means the traffic is being mirrored to the FTD.

The next step is to set up an intrusion policy that defines the rules and actions for detecting and responding to malicious traffic.

Steps:

In FMC, navigate to Policies > Intrusion.

Create a new intrusion policy or edit an existing one.

Define the rules and actions for detecting threats.

Apply the intrusion policy to the relevant interfaces or access control policies.

This configuration enables the FTD to inspect the mirrored traffic and take appropriate actions based on the defined intrusion policy.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Intrusion Policies.

質問: 196

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

- A. Cisco Firepower Threat Defense モード
- B. ルーテッド モード
- C. ルーティングとブリッジングの統合
- D. 透過モード

正解: ([正解を表示します](#))

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

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**3 0 %ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 197

エンジニアは、Cisco FMC を使用して、ネットワーク経由で送信されているファイルがマルウェアかどうかを判断するように指示されています。このファイル検索を実行するには、どの 2 つの構成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. Cisco FMC は、サンドボックス化のために Cisco ThreatGrid サービスに直接接続する必要があります。
- 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. Cisco FMC はマルウェア検索のためのファイル検査ポリシーを含める必要があります。
- D. Cisco FMC に SSL 復号化ポリシーを含める必要があります。
- E. Cisco FMC は FireAMP クラウドに接続する必要があります。

正解: ([正解を表示します](#))

質問: 198

ネットワーク管理者は、Cisco Secure Firewall Management Centerで過去24時間に行った変更の詳細を記載した日次メールレポートを経営陣に送信する必要があります。この要件を満たすには、どのシステム設定を有効にする必要がありますか？

- A. 変更調整
- B. HTTPサーバーに監査ログを送信する
- C. 監査ログをSyslogに送信する
- D. STIG準拠

正解: [\(正解を表示します\)](#)

Change Reconciliation records snapshots whenever users save system-configuration changes and combines those snapshots into a detailed report covering the previous 24 hours. Under System > Configuration > Change Reconciliation, the administrator enables the feature, selects the daily execution time, and specifies management's recipient email addresses. The administrator can also include policy-configuration changes and enable the full change history instead of receiving only a consolidated view. An email relay host must be configured so that Management Center can deliver the report. Sending audit logs to an HTTP or syslog server streams audit events to an external collector; it does not generate the required daily email summary. STIG Compliance applies security-hardening settings and is unrelated to scheduled change reporting. Cisco Change Reconciliation documentation

質問: 199

展示資料を参照してください。

```
S1# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled
Codes: > - best, < - connected, S - static
C 192.168.20.0/24 is directly connected, vlan 10
```

エンジニアは、Cisco Catalyst スイッチで静的ルートを設定して、192.168.10.0/24 に到達する必要があります。

ネクストホップは192.168.20.1です。ルートは管理距離2を使用する必要があります。どのコマンドが要件を満たしますか？

- A. ip route 192.168.10.0 255.255.255.0 192.168.20.1 1
- B. ip route 192.168.20.0 255.255.255.0 192.168.10.1 1
- C. ip route 192.168.10.0 255.255.255.0 192.168.20.1 2
- D. ip route 192.168.20.0 255.255.255.0 192.168.10.1 2

正解: **C** ([コメントを发表する](#))

A static-route command follows the structure ip route destination-network subnet-mask next-hop administrative-distance. The required destination is 192.168.10.0/24, which corresponds to subnet mask 255.255.255.0. The next-hop address must be 192.168.20.1, and the routing-table exhibit confirms that the 192.168.20.0/24 network is directly connected through VLAN 10. The final value must be 2 because the question explicitly requires an administrative distance of 2. Option A uses the correct destination and next hop but sets the distance to 1. Options B and D incorrectly reverse the destination and next-hop networks.

Consequently, only option C contains all four required elements and installs the route through the connected 192.168.20.0/24 network with the specified preference.

質問: 200

Cisco Secure Firewall Management Center で管理されているデバイスで、2 人のユーザーが同時に VPN ポリシーを変更すると、どのような結果になりますか？

- A. 両方のユーザーがポリシーを編集でき、最後に保存された構成が保持されます。
- B. 最初のユーザーがポリシーの編集を選択すると、構成がロックされます。
- C. 両方のユーザーによる変更がポリシーにマージされます。
- D. システムは、複数のユーザーによるポリシーの変更を防止します。

正解: **B** ([コメントを發表する](#))

In Cisco Secure Firewall Management Center (FMC), when two users attempt to modify a VPN policy simultaneously, the system implements a locking mechanism to prevent conflicts. The first user who selects edit on the policy locks the configuration, preventing other users from making changes until the lock is released.

Steps:

When the first user selects edit on the VPN policy, FMC locks the policy for editing.

The lock ensures that only the first user can make changes.

Once the first user saves or cancels their changes, the lock is released.

Other users can then edit the policy.

This locking mechanism ensures that configuration conflicts are avoided and only one set of changes is applied at a time.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Policy Management and User Permissions.

質問: **201**

エンジニアが2番目のCiscoFMCをスタンバイデバイスとして設定していますが、アクティブユニットに登録できません。この問題の原因は何ですか？

- A. プライマリFMCには、現在デバイスが接続されています。
- B. CiscoFMCデバイスで実行されているコードバージョンが異なります
- C. 購入したライセンスには高可用性が含まれていません
- D. 2つのデバイス間の帯域幅はわずか10Mbpsです。

正解: ([正解を表示します](#))

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

質問: **202**

エンジニアが新しいFirepower展開をセットアップし、実装を開始するためのデフォルトのFMCポリシーを検討しています。最初の試用段階で、組織は、ネットワークトラフィックの大部分が通過できるようにしながら、いくつかの一般的なSnortルールをテストしたいと考えています。利用される？

- A. 最大検出
- B. 接続を介したセキュリティ
- C. バランスの取れたセキュリティと接続性
- D. セキュリティを介した接続

正解: ([正解を表示します](#))

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

質問: **203**

パケットキャプチャのトレースオプションを選択する利点は何ですか？

- A. 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。
- B. 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. オプションは、各パケットの詳細をキャプチャします。
- D. オプションは、宛先ホストが別のパスを介して応答するかどうかを示しました。

正解: ([正解を表示します](#))

質問: 204

ネットワーク上のトラフィック量が増加しており、コンプライアンス上の理由から、管理者は暗号化されたトラフィックを可視化する必要があります。TLSのSSL復号化を有効にしてこの可視性を実現した結果はどうなりますか？

- A. プライバシー規制の対象ではありません
- B. パフォーマンスへの影響は最小限です
- C. 企業が管理する証明書の必要性を促します
- D. 証明書のピン留めが強制されていない場合は失敗します

正解: ([正解を表示します](#))

質問: 205

エンドポイントで重大な脅威を検出すると、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Cisco Identity ServicesEngine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. Cisco ASA 5500 Series
- B. Cisco ASR 7200 Series
- C. Cisco FMC
- D. Cisco AMP
- E. Cisco Stealthwatch

正解: ([正解を表示します](#))

質問: 206

エンジニアは、組織のプライマリ Cisco FMC の災害復旧を担当しています。

プライマリ Cisco FMC が故障した場合に元の企業ポリシーのコピーが利用できるようにするために、プライマリおよびセカンダリ Cisco FMC で何をする必要がありますか？

- A. プライマリおよびセカンダリ Cisco FMC の両方で高可用性を構成します。
- B. プライマリ デバイスが故障したときに、プライマリ Cisco FMC のバックアップ構成をセカンダリ Cisco FMC デバイスに復元します。
- C. アクティブな Cisco FMC デバイスを、スタンバイ デバイスと同じ信頼できる管理ネットワークに配置します。
- D. プライマリおよびセカンダリ Cisco FMC デバイスを、長さ 10 メートル以下のカテゴリ 6 ケーブルで接続します。

正解: **B** ([コメントを發表する](#))

質問: 207

ネットワークセキュリティエンジニアは、問題のトラブルシューティング中に、Cisco FMC Webブラウザ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/CAP/pcap/test.pcap にアクセスすると、PCAPファイルの代わりにエラー403 :アクセス禁止が表示されました。この問題を解決するために、エンジニアはどのような対応を取る必要がありますか？

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

正解: ([正解を表示します](#))

有効的な**300-710J**問題集はJPNTTest.com提供され、**300-710J**試験に合格することに役に立ちます！JPNTTest.comは今最新**300-710J**試験問題集を提供します。JPNTTest.com 300-710J試験問題集はもう更新されました。ここで**300-710J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/300-710J-mondaishu> **446**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」