Securing Networks with Cisco Firepower (300-710 Japanese Version)

1. アナリストは、その週のCiscoFMCレポートを確認しています。彼らは、いくつかのピアツーピアアプリケーションがネットワーク上で使用されていることに気づき、環境に最大のリスクをもたらすものを特定する必要があります。アナリストにこの情報を提供するレポートはどれですか？

A. ネットワークリスクレポート

B. 攻撃リスクレポート

C. ユーザーリスクレポート

D. 高度なマルウェアリスクレポート

Answer(s): A

---

2. 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。

Answer(s): D

---

3. 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. Cisco AMP for Networks

B. file policies

C. Cisco AMP for Endpoints

D. intrusion and file events

Answer(s): A

---

4. 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

Answer(s): C

---

5. エンジニアがネットワークにCiscoFTDを実装し、使用するFirepowerモードを決定しています。組織では、トラフィックセグメンテーションを提供するためにFTDアプライアンス内で複数の仮想Firepowerデバイスを個別に動作させる必要があります。これらの要件をサポートするには、Cisco Firepower ManagementConsoleでどの展開モードを設定する必要がありますか。

A. 複数の展開

B. マルチインスタンス

C. シングルコンテキスト

D. 単一展開

Answer(s): B

---

6. 病院ネットワークは、Cisco FMC管理対象デバイスをアップグレードする必要があり、ディザスタリカバリプロセスが実施されていることを確認する必要があります。ネットワークのダウンタイムを最小限に抑えるために何をする必要がありますか？

A. バックアップとして使用するために現在の構成のコピーを保持します

B. フェールオーバー用にCiscoFMCを設定します

C. 冗長性を追加するためにISPへの2番目の回線を構成します

D. CiscoFMC管理対象デバイスをクラスタリング用に設定します。

Answer(s): A

---

7. Cisco FMCで再利用可能でサポートされているオブジェクトの2つのタイプはどれですか。（2つ選択してください。）

A. レイヤー7アプリケーションプロトコルへのHTTPおよびHTTPS GETリクエストのリンクに役立つ動的キーマッピングオブジェクト。

B. セキュリティインテリジェンスのフィードとリストを表すレピュテーションベースのオブジェクト、カテゴリとレピュテーションに基づくアプリケーションフィルター、およびファイルリスト

C. IPアドレスとネットワーク、ポート/プロトコルのペア、VLANタグ、セキュリティゾーン、および送信元/送信先の国を表すネットワークベースのオブジェクト

D. FQDNマッピングとネットワーク、ポート/プロトコルのペア、VXLANタグ、セキュリティゾーン、および送信元/送信先の国を表すネットワークベースのオブジェクト

E. URLカテゴリなどの評判ベースのオブジェクト

Answer(s): B,C

---

8. 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. マルウェアのアクションと動的分析をブロックする

B. マルウェアクラウドルックアップと動的分析

C. 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

D. 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

Answer(s): D

---

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

A. 時間範囲

B. セキュリティグループタグ

C. ネットワークオブジェクト

D. DNSサーバーグループ

Answer(s): C

---

10. 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. 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。

C. ハッシュを単純なカスタム検出リストに追加します。

D. 感染したエンドポイントでパーソナルファイアウォールを有効にします。

Answer(s): C

---

11. ネットワークセキュリティエンジニアは、障害のあるCiscoFTDデバイスをハイアベイラビリティペアで交換する必要があります。故障したユニットを交換する際に取らなければならないアクションはどれですか？

A. 障害のあるCiscoFTDデバイスをCiscoFMCから登録解除します

B. 交換用ユニットの電源を入れる前に、アクティブなCiscoFTDデバイスをシャットダウンします。

C. 障害のあるCiscoFTDデバイスがCiscoFMCに登録されたままであることを確認します。

D. 交換用ユニットの電源を入れる前に、CiscoFMCをシャットダウンしてください。

Answer(s): A

---

12. ネットワーク エンジニアは、既存のファイアウォールを NAT 構成に設定する必要があります。現在の構成では、コンテキストごとに 2 つ以上のインターレースをサポートする必要があります。ファイアウォールは、以前は透過モードで動作していました。Cisco Secure Firewall Throat Defense (FTD) デバイスは、Cisco Secure Firewall Management Center (FMC) から登録解除されました。要件を満たすために、ネットワーク エンジニアが次に実行する必要がある構成アクションのセットは何ですか。

A. Secure FTD デバイス CL1 から configure manager add routed コマンドを実行し、Secure FMC に再登録します。

B. Secure FTD デバイス CD から configure firewall routed コマンドを実行し、Secure FMC に再登録します。

C. Secure FMC CLI から configure manager add routed コマンドを実行し、Secure FMC に再登録します。

D. Secure FMC CLI から configure firewall routed コマンドを実行し、Secure FMC に再登録します。

Answer(s): B

---

13. セキュリティエンジニアが従業員の電子メールアドレスから疑わしいファイルを見つけ、分析のためにアップロードしようとしていますが、アップロードに失敗しています。最後の登録ス

テータスはまだアクティブです。この問題の原因は何ですか？

A. Cisco AMP for Networksは、オンプレミスでCisco ThreatGridに接続できません。

B. ホスト制限が設定されています。

C. Cisco AMP forNetworksはCiscoThreat GridCloudに接続できません。

D. ユーザーエージェントのステータスは監視するように設定されています。

Answer(s): C

---

14. 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

Answer(s): D

---

15. 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. ルールで誤ったアプリケーション署名が使用されました。

B. ルールは作成後に有効化されませんでした。

C. Snort の間違ったソース インターフェイスがルールで選択されました。

D. ルールに対してロギングが有効になっていません。

Answer(s): B

---

16. ネットワーク ユーザーは、別のネットワーク セグメントにあるサーバーにアクセスするときに問題が発生します。エンジニアは、Cisco Secure Firewall Threat Defense でパケット キャプチャを実行して問題を調査します。エンジニアは、より多くのデータを期待しており、15 分間のキャプチャできないセッション中にすべてのトラフィックが収集されたわけではないと考えています。

A. キャプチャしたデータをFTPサーバーに転送する

B. キャプチャに割り当てられる RAM の量を増やします。

C. データを保存するファイル名を指定します。

D. 割り当てられたメモリが十分であることを確認します。

Answer(s): D

---

17. 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

Answer(s): C

---

18. 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

Answer(s): A,C

---

19. エンジニアは、8699 / udpを介してサーバーに接続する必要がある一部のデバイスのトラフィックを許可するように要求するチケットを確認しています。リクエストには1つのIPアドレス172.16.18.15のみが記載されていますが、リクエスターはエンジニアに、先週接続を試みたすべてのマシンのポートを開くように要求しました。この問題のトラブルシューティングを行うには、エンジニアはどのアクションを実行する必要がありますか？

A. コンテキストエクスプローラーを使用して、宛先ポートブロックを確認します

B. 送信元ポート8699 / udpで接続イベントをフィルタリングします。

C. 宛先ポート8699 / udpで接続イベントをフィルタリングします。

D. コンテキストエクスプローラーを使用して、プロトコルごとのアプリケーションブロックを確認します。

Answer(s): C

---

20. 組織は、HTTPトラフィックをブロックするときにデフォルトのCiscoFirepowerブロックページを使用することを望んでいません。組織は、ブロックが発生するたびにユーザーを教育するのに役立つ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実行する必要がある2つのステップはどれですか？（2つ選択してください。）

A. ポリシーと手順の情報を使用してHTMLコードを作成します。

B. アクセス制御ポリシーのHTTPリクエスト処理をカスタマイズされたブロックに編集します。

C. 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。

D. ポリシーと手順の情報を含むCSSコードを記述します。

E. アクセス制御ポリシーのHTTP応答をカスタムに変更します。

Answer(s): A,E
