

Cisco.350-701.v2022-08-23.q531

試験コード：	350-701
試験名称：	Implementing and Operating Cisco Security Core Technologies
認証ベンダー：	Cisco
無料問題の数：	531
バージョン：	v2022-08-23
ページの閲覧量：	809
問題集の閲覧量：	38556

<https://www.jpnsiken.com/shiken/Cisco.350-701.v2022-08-23.q531.html>

質問: 1

エンドポイント向けの十分に確立されたパッチソリューションがない場合、企業が脆弱になる2つのリスクはどれですか。2つ選択してください)

- A. エクスプロイト
- B. ARPスプーフィング
- C. サービス拒否攻撃
- D. マルウェア
- E. 盗聴

正解: A,D ([コメントを发表する](#))

説明

マルウェアとは、悪意のあるソフトウェア」を意味し、コンピューター、サーバー、クライアント、またはコンピューターネットワークに損害を与えるように意図的に設計されたソフトウェアです。最も一般的な種類のマルウェアには、ウイルス、ランサムウェア、スパイウェアが含まれます。ウイルスおそらく最も一般的なタイプのマルウェアであるウイルスは、悪意のあるコードを添付してコードをクリーンアップし、実行されるのを待ちます。

ランサムウェアは、コンピューターに感染し、システムが再び機能するために料金の支払いを要求するメッセージを表示する悪意のあるソフトウェアです。

スパイウェアは、コンピューターやモバイルデバイスに入力、アップロード、ダウンロード、保存するすべてのものを密かに記録できるスパイソフトウェアです。スパイウェアは常に自分自身を隠そうとします。

エクスプロイトは、ソフトウェアの脆弱性またはセキュリティ上の欠陥を利用するコードです。

エクスプロイトとマルウェアは、最新ではないエンドポイントの2つのリスクです。ARPスプーフィングと盗聴はネットワークに対する攻撃ですが、サービス拒否攻撃はIPパケットのフラッディングに基づいています。

質問: 2

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

質問: 3

モールドは、共有アプライアンスを使用して顧客にセキュリティサービスを提供します。モールドは、共有アプライアンスの管理を分離することを望んでいます。これらのニーズを満たすASAデプロイメントモードはどれですか？

- A. ルーテッドモード
- B. マルチゾーンモード
- C. マルチコンテキストモード
- D. 透過モード

正解: (正解を表示します)

質問: 4

Cisco FTDエンジニアは、組織用にs2s00123456789と呼ばれる新しいIKEv2ポリシーを作成して、追加のプロトコルでネットワークデバイスを終端できるようにしています。現在、確立されているポリシーは1つだけであり、一部のデバイスがプライマリポリシーにリストされているより強力なアルゴリズムをサポートできない場合に備えて、新しいポリシーをバックアップにする必要があります。これをサポートするために何をすべきですか？

- A. 整合性アルゴリズムをSHA *に変更して、プライマリポリシーですべてのSHAアルゴリズムをサポートします
- B. 新しいポリシー5とプライマリポリシー1を優先します
- C. 暗号化をAES *に変更して、プライマリポリシーのすべてのAESアルゴリズムをサポートします

D. プライマリポリシー10と新しいポリシー1を優先します

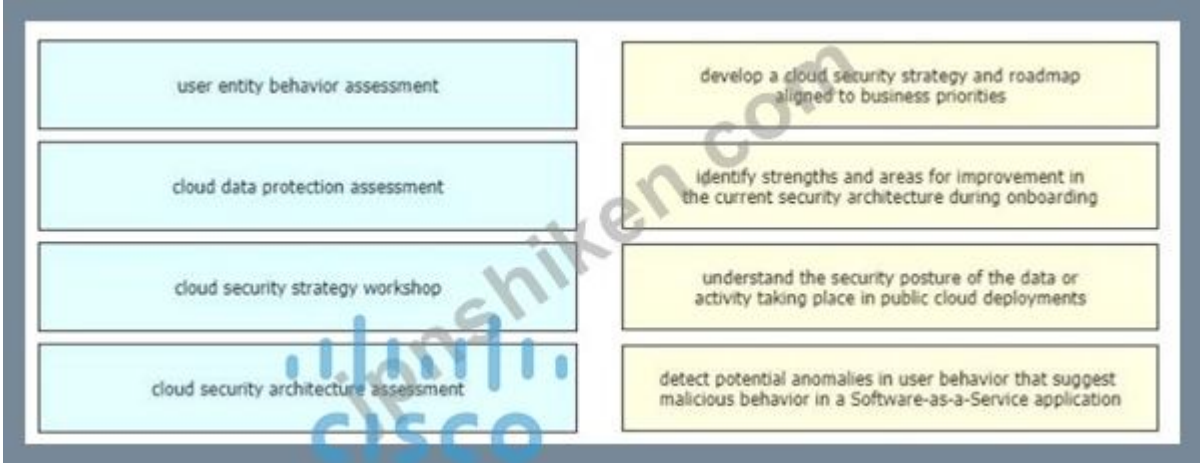
正解: [\(正解を表示します\)](#)

選択したポリシーセクションの内容に関係なく、デバイス上のすべてのIKEポリシーがリモートピアに送信されます。
リモートピアによって一致した最初のIKEポリシーが、VPN接続用に選択されます。優先度フィールドを使用して、最初に送信するポリシーを選択します。優先度1が最初に送信されます。
選択したポリシーセクションの内容に関係なく、デバイス上のすべてのIKEポリシーがリモートピアに送信されます。
リモートピアによって一致した最初のIKEポリシーが、VPN接続用に選択されます。優先度フィールドを使用して、最初に送信するポリシーを選択します。優先度1が最初に送信されます。

参照：
選択したポリシーセクションの内容に関係なく、デバイス上のすべてのIKEポリシーがリモートピアに送信されます。
リモートピアによって一致した最初のIKEポリシーが、VPN接続用に選択されます。優先度フィールドを使用して、最初に送信するポリシーを選択します。優先度1が最初に送信されます。

質問: 5

クラウドセキュリティ評価コンポーネントを左側から右側の定義にドラッグアンドドロップします。



正解:



質問: 6

悪意のあるユーザーが、4つの異なるスイッチポートで同時にMABを使用して許可されたプリンタ接続をスプーフィングすることにより、ネットワークアクセスを取得しました。それ以上の違反を防ぐ2つの触媒スイッチセキュリティ機能はどれですか？ 2つ選択してください)

- A. DHCPスヌーピング
- B. プライベートVLAN
- C. 802.1AE MacSec
- D. ポートセキュリティ
- E. IPデバイストラック
- F. 動的ARP検査

正解: ([正解を表示します](#))

質問: 7

Cisco ASA NetFlow v9セキュアイベントロギングの特徴は何ですか？

- A. フロー作成、フローティアダウン、およびフロー拒否のイベントを追跡します。
- B. 特定のフローのすべてのレコードをエクスポートするステートレスIPフロー追跡を提供します。
- C. フローを継続的に追跡し、10秒ごとに更新を提供します。
- D. そのイベントはすべてのトラフィッククラスに並行して一致します。

正解: ([正解を表示します](#))

説明/リファレンス <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.html>

質問: 8

Cisco Umbrellaでブラックリストに登録されるように指定されている個々のサイトはどこにありますか？

- A. アプリケーション設定
- B. コンテンツカテゴリ
- C. セキュリティ設定
- D. 宛先リスト

正解: D ([コメントを发表する](#))

宛先リストは、組織内のIDに適用されるポリシーの管理設定に基づいてブロックまたは許可できるインターネット宛先のリストです。宛先は、IPアドレス (IPv4)、URL、または完全修飾ドメイン名です。宛先リストはいつでもUmbrellaに追加できます。ただし、宛先リストは、ポリシーに追加されるまで使用されません。参照 <https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists>組織内のIDに適用されるポリシーの設定。宛先は、IPアドレス (IPv4)、URL、または完全修飾ドメイン名です。宛先リストはいつでもUmbrellaに追加できます。ただし、宛先リストは、ポリシーに追加されるまで使用されません。

宛先リストは、組織内のIDに適用されるポリシーの管理設定に基づいてブロックまたは許可できるインターネット宛先のリストです。宛先は、IPアドレス (IPv4)、URL、または完全修飾ドメイン名です。宛先リストはいつでもUmbrellaに追加できます。ただし、宛先リストは、ポリシーに追加されるまで使用されません。参照 <https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists>

質問: 9

Cisco AnyConnect VPNを使用するときに、最も強力なスループットパフォーマンスを提供するプロトコルはどれですか。

- A. BJTLSv1
- B. DTLSv1
- C. TLSv1.2

D. TLSv1.1

正解: ([正解を表示します](#))

質問: 10

SQLインジェクションの脆弱性を悪用する場合、攻撃者はどの欠陥を利用しますか？

A. WebページまたはWebアプリケーションでのユーザー入力の検証

B. LinuxおよびWindowsオペレーティングシステム

C. データベース

D. ウェブページの画像

正解: ([正解を表示します](#))

説明

SQLインジェクションは通常、ユーザー名/ユーザーIDなどの入力をユーザーに求めるときに発生しますが、ユーザーはデータベースで無意識のうちに実行するSQLステートメントをユーザーに提供（「インジェクション」）します。例えば：

次の例を見てください。この例では、変数 `txtUserId` を選択文字列に追加してSELECTステートメントを作成しています。変数はユーザー入力（`getRequestString`）からフェッチされます。

```
txtUserId = getRequestString ("UserId");
```

```
txtSQL = "SELECT * FROM Users WHERE UserId =" + txtUserId;
```

ユーザーが「100OR1= 1」のように入力すると、SQLステートメントは次のようになります。

```
SELECT * FROM Users WHERE UserId = 100 OR 1 = 1;
```

上記のSQLは有効であり、OR 1 = 1は常にTRUEであるため、「Users」テーブルからすべての行を返します。ハッカーは、このデータベース内のすべてのユーザー名とパスワードにアクセスする可能性があります。

質問: 11

データプレーン通信に暗号化と認証を提供するアルゴリズムはどれですか？

A. AES-GCM

B. SHA-96

C. AES-256

D. SHA-384

正解: ([正解を表示します](#))

ネットワークのデータプレーンは、ネットワークを介して転送されるデータパケットを処理する責任があります。データプレーンはフォワーディングプレーンと呼ばれることもあります。）多分これはSD-WANネットワークのデータプレーンでの暗号化と認証について質問したいです（しかしSD-WANはSCOR 350-701試験のトピックではありませんか？）。ユニキャストトラフィック用のCiscoSD-WANネットワークでは、データプレーンの暗号化はAES-256-GCMによって行われます。これは、同じキーを使用して発信パケットを暗号化し、着信パケットを復号化する対称キーアルゴリズムです。各ルーターは、データパスのAESキー（具体的には、TLOCごとに1つのキー）を定期的に生成し、IPルートの更新と同様に、このキーをOMPルートパケットでvSmartコントローラーに送信します。参照 <https://www.cisco.com>。

ユニキャストトラフィック用のCiscoSD-WANネットワークでは、データプレーンの暗号化はAES-256-GCMによって行われます。これは、同じキーを使用して発信パケットを暗号化し、着信パケットを復号化する対称キーアルゴリズムです。各ルーターは、データパスのAESキー（具体的には、TLOCごとに1つのキー）を定期的に生成し、IPルートの更新と同様に、このキーをOMPルートパケットでvSmartコントローラーに送信します。

ネットワークのデータプレーンは、ネットワークを介して転送されるデータパケットを処理する責任があります。データプレーンはフォワーディングプレーンと呼ばれることもあります。）多分これはSD-WANネットワークのデータプレーンでの暗号化と認証について質問したいです（しかしSD-WAN

はSCOR 350-701試験のトピックではありませんか？)。ユニキャストトラフィック用のCiscoSD-WANネットワークでは、データプレーンの暗号化はAES-256-GCMによって行われます。これは、同じキーを使用して発信パケットを暗号化し、着信パケットを復号化する対称キーアルゴリズムです。各ルーターは、データパスのAESキー（具体的には、TLOCごとに1つのキー）を定期的に生成し、IPルートの更新と同様に、このキーをOMPルートパケットでvSmartコントローラーに送信します。参照 <https://www.cisco.com>。

質問: 12

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides the ability to perform network discovery

provides intrusion prevention before malware compromises the host

Cisco Firepower

Cisco AMP

正解:

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides the ability to perform network discovery

provides intrusion prevention before malware compromises the host

Cisco Firepower

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides the ability to perform network discovery

provides superior threat prevention and mitigation for known and unknown threats

Cisco AMP

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides intrusion prevention before malware compromises the host

質問: 13

Cisco DNA Centerは、ネットワークを完全に制御するためにどのタイプのダッシュボードを提供しますか？

- A. サービス管理
- B. 集中管理
- C. アプリケーション管理

D. 分散管理

正解: [\(正解を表示します\)](#)

シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。
シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。
シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。

質問: 14

展開内の他の管理対象デバイスと類似している可能性が高い管理対象デバイスの側面を定義する機能またはパラメーターの共有セットを表すポリシーはどれですか？

- A. グループポリシー
- B. アクセス制御ポリシー
- C. デバイス管理ポリシー
- D. プラットフォームサービスポリシー

正解: [\(正解を表示します\)](#)

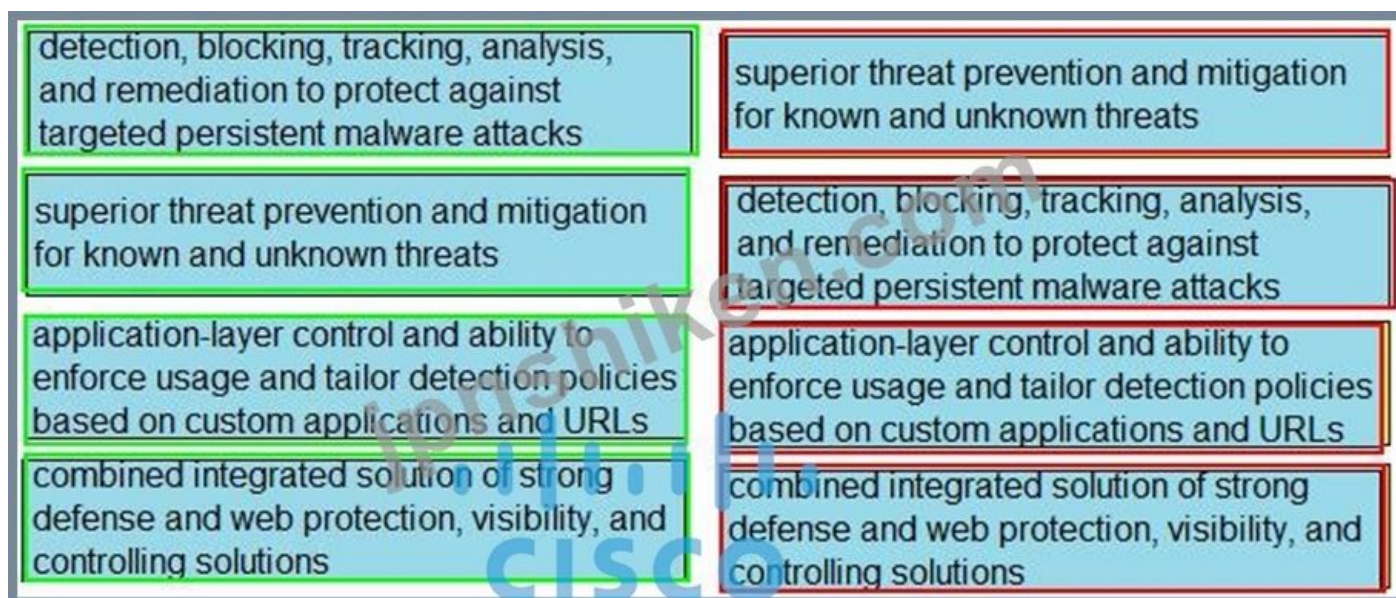
説明/リファレンス https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/platform_settings_policies_for_managed_devices.pdf

質問: 15

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:



質問: 16

組織は最近CiscoWSAをインストールし、AVCエンジンを利用して、組織がアプリケーション固有のアクティビティを制御するためのポリシーを作成できるようにしたいと考えています。AVCエンジンを有効にした後、これを実装するには何をする必要がありますか？

- A. Webセキュリティレポートを使用してエンジン機能を検証する
- B. セキュリティサービスを使用してトラフィックモニターを構成します。
- C. URL分類を使用して、アプリケーショントラフィックを防止します。
- D. アクセスポリシーグループを使用して、アプリケーション制御設定を構成します。

正解: D ([コメントを发表する](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

NetFlowフローで定義されている2つのフィールドはどれですか？ 2つ選択してください)

- A. サービスバイトのタイプ
- B. サービスクラスビット
- C. レイヤー4プロトコルタイプ
- D. 宛先ポート
- E. 出力論理インターフェース

正解: ([正解を表示します](#))

シスコの標準NetFlowバージョン5は、フローを、フローの一意のキーを定義する7つの値をすべて共有するパケットの単方向シーケンスとして定義しています。

+入力インターフェイス \$NMP ifIndex)

+送信元IPアドレス

- +宛先IPアドレス
- + IPプロトコル
- + UDPまたはTCPの場合は送信元ポート、その他のプロトコルの場合は0
- + UDPまたはTCPの場合は宛先ポート、ICMPの場合はタイプとコード、その他のプロトコルの場合は0
- + IPタイプオブサービス

注 :フローは、特定の送信元と宛先の間の単方向の一連のパケットです。

質問: 18

IaaSクラウドサービスモデルでは、プロバイダーが管理を担当するセキュリティ機能はどれですか？

- A. インターネットプロキシ
- B. 仮想マシンのファイアウォール
- C. CASB
- D. ハイパーバイザーOSの強化

正解: ([正解を表示します](#))

クラウドコンピューティングのIaaS (Infrastructure as a Service)は、最も重要で最も急速に成長している分野の1つです。このサービスモデルでは、クラウドプロバイダーは、仮想マシンとしてのコンピューター、raw (ブロック)ストレージ、ファイアウォール、ロードバランサー、およびネットワークデバイスを含むユーザー/マシンにリソースを提供します。

質問: 19

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

質問: 20

Cisco Threat Intelligence Directorと統合して、セキュリティの脅威に関する情報を提供し、SOCがそれらの脅威への対応をプロアクティブに自動化できるようにするものは何ですか。

- A. Cisco Umbrella
- B. 外部脅威フィード
- C. Cisco Threat Grid
- D. Cisco Stealthwatch

正解: **C** ([コメントを发表する](#))

説明CiscoThreatIntelligence Director (CTID)は、組織によって展開されている既存の脅威インテリジェンスプラットフォームと統合して、脅威インテリジェンスを自動的に取り込むことができます。参照 <https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector> Cisco Threat Intelligence Director (CTID)は、組織によって展開されている既存の脅威インテリジェンスプラットフォームと統合して、脅威インテリジェンスを取り込むことができます。自動的。

説明CiscoThreatIntelligence Director (CTID)は、組織によって展開されている既存の脅威インテリジェンスプラットフォームと統合して、脅威インテリジェンスを自動的に取り込むことができます。参照 <https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector>

質問: 21

エンジニアは、ネットワーク上のトラフィックの中断に気づきます。さらに調査すると、ブロードキャストパケットがネットワークにフラッディングしていることがわかりました。この問題に対処するには、事前定義されたしきい値に基づいて何を構成する必要がありますか？

- A. Bridge Protocol Data Unit Guard
- B. 組み込みイベントの監視
- C. アクセス制御リスト
- D. ストームコントロール

正解: ([正解を表示します](#))

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e1.html>

質問: 22

エンジニアはネットワーク内にNTP認証を実装しており、コマンドntp authentication-key 1md5Cisc392368270を使用してクライアントデバイスとサーバーデバイスの両方を設定しました。1.1.1.1のサーバーは、1.1.1.2のクライアントに対して認証を試みていますが、認証できません。クライアントがサーバーの認証キーを受け入れることができるようにするには、どのコマンドが必要ですか？

- A. ntpピア1.1.1.1キー1

- B. ntpサーバー1.1.1.1キー1
- C. ntpサーバー1.1.1.2キー1
- D. ntpピア1.1.1.2キー1

正解: [\(正解を表示します\)](#)

説明

説明

他のデバイスがルーターに接続するときに認証を要求するようにNTP対応ルーターを構成するには、次のコマンドを使用します。

NTP_Server (config)#ntp authentication-key 2 md5 securitytut

NTP_Server (config)#ntp authenticate

NTP_Server (config)#ntp trusted-key 2

次に、クライアントルータで同じ認証キーを設定する必要があります。

NTP_Client (config)#ntp authentication-key 2 md5 securitytut

NTP_Client (config)#ntp authenticate

NTP_Client (config)#ntp trusted-key 2

NTP_Client (config)#ntp server 10.10.10.1 key 2

注 :CiscoデバイスをNTPクライアントとして設定するには、コマンドntpserver<IPアドレス>を使用します。例えば :

Router (config)#ntpserver10.10.0.1。このコマンドは、時間について10.10.10.1を照会するようにルーターに指示します。

質問: 23

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

質問: 24

脅威分析のためにプリロードされた行動指標に対してファイルの自動化された静的および動的分析を実行するプロセスは何ですか？

- A. 深い可視性スキャン
- B. 高度なサンドボックス
- C. 高度なスキャン
- D. ポイントインタイムチェック

正解: B ([コメントを发表する](#))

質問: 25

エンジニアはCiscoUmbrellaで新しいネットワークIDを設定しましたが、トラフィックがCiscoUmbrellaネットワークを介してルーティングされていることを確認する必要があります。

ルーティングをテストするアクションはどれですか？

- A. クライアントコンピューターがオンプレミスのDNSサーバーを指していることを確認します。
- B. インテリジェントプロキシを有効にして、トラフィックが正しくルーティングされていることを検証します。
- C. クライアントコンピューターの背後にあるパブリックIPアドレスをコアIDに追加します。
- D. <http://welcome.umbrella.com/>にアクセスして、新しいIDが機能していることを確認します。

正解: ([正解を表示します](#))

説明/参照 :

質問: 26

DMVPNを介したCiscoAny接続を使用する2つの利点は何ですか。2つ選択してください。)

- A. さまざまなルーティングプロトコルがトンネル上で機能できるようにします
- B. ユーザーIDに基づいてアクセスポリシーをカスタマイズできます
- C. 複数のサイトがデータセンターに接続できるようにします
- D. マシンからの個々のユーザーのVPNアクセスを可能にします
- E. ハブを通過せずにスポークツースポーク通信を提供します

正解: B,D ([コメントを发表する](#))

質問: 27

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

正解:

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

uses six packets in main mode to establish phase 1

uses three packets in aggressive mode to establish phase 1

IKEv2

standard includes NAT-T

uses four packets to establish phase 1 and phase 2

uses EAP for authenticating remote access clients

質問: 28

展示を参照してください。

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                  = AUTHENTICATOR
PortControl          = FORCE_AUTHORIZED
ControlDirection     = Both
HostMode             = SINGLE_HOST
QuietPeriod          = 60
ServerTimeout        = 0
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30
```

この出力を表示するために使用されたコマンドはどれですか？

- A. show dot1x interface gi1 / 0/12
- B. dot1xのすべての概要を表示
- C. dot1xallを表示
- D. dot1xを表示

正解: ([正解を表示します](#))

質問: 29

エンジニアはCiscoUmbrellaで新しいネットワークIDを設定しましたが、トラフィックがCiscoUmbrellaネットワークを介してルーティングされていることを確認する必要があります。ルーティングをテストするアクションはどれですか？

- A. クライアントコンピューターの背後にあるパブリックIPアドレスをコアIDに追加します。
- B. クライアントコンピューターがオンプレミスのDNSサーバーを指していることを確認します。
- C. 参照

<http://welcome.umbrella.com/>にアクセスして、新しいIDが機能していることを確認します。

- D. インテリジェントプロキシを有効にして、トラフィックが正しくルーティングされていることを検証します。

正解: ([正解を表示します](#))

質問: 30

CI / CDパイプラインへの安全なアクセスのためにどのソリューションを活用する必要がありますか？

- A. Duo Network Gateway
- B. SSL WebVPN
- C. CiscoFTDネットワークゲートウェイ
- D. リモートアクセスクライアント

正解: ([正解を表示します](#))

質問: 31

VPNに接続していないときにリモートユーザーをフィッシング攻撃から保護するシスコのセキュリティソリューションはどれですか。

- A. Cisco Stealthwatch
- B. Cisco Umbrella
- C. Cisco Firepower
- D. NGIPS

正解: ([正解を表示します](#))

説明

Cisco Umbrellaは、接続が確立される前に、安全でない宛先を事前に分析してブロックすることにより、悪意のあるドメインへのアクセスからユーザーを保護します。したがって、攻撃者が送信した特定のリンクをクリックしたときに疑わしいドメインをブロックすることで、フィッシング攻撃から保護できます。Cisco Umbrellaローミングは、VPNを使用していない場合でも従業員を保護します。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

欺瞞的なフィッシングとスパフィッシングの違いは何ですか？

- A. スパフィッシングとは、攻撃が組織のCレベルの幹部を狙ったものである場合です。
- B. 詐欺的なフィッシングは、被害者のDNSサーバーを乗っ取って操作し、ユーザーを偽のWebページにリダイレクトします。
- C. 詐欺的なフィッシングは、Cレベルの役割を持つ組織内の特定のユーザーを狙った攻撃です。
- D. スパフィッシングキャンペーンは、特定の個人とグループの人々を対象としています。

正解: ([正解を表示します](#))

質問: 33

CiscoISRがデフォルトのバイパスリストをWebフィルタリングに自動的に使用できるようにする機能はどれですか。

- A. フィルター
- B. コネクタ
- C. 会社の鍵
- D. グループキー

正解: B ([コメントを发表する](#))

質問: 34

どのアルゴリズムが非対称暗号化を提供しますか？

- A. RC4
- B. RSA
- C. AES
- D. 3DES

正解: ([正解を表示します](#))

参照 :

<https://securityboulevard.com/2020/05/types-of-encryption-5-encryption-algorithms-how-to-choose-the-right-one/#:~:text=Standard%20asymmetric%20encryption%20algorithms%20include,%2C%20El%20Gamal%2C%20and%20DSA。>

質問: 35

組織は、ネットワーク上にマイクロセグメンテーションを実装しようとしており、ネットワーク内のアプリケーションの可視性を取得できるようにしたいと考えています。ソリューションは、コンプライアンスを維持および強制できる必要があります。これらの要件を満たすためにどの製品を使用する必要がありますか？

- A. Cisco Umbrella
- B. Cisco AMP
- C. Cisco Stealthwatch
- D. Cisco Tetration

正解: ([正解を表示します](#))

マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照 :<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf>は他のすべてのトラフィックを拒否します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。

Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。

正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーショ

ンに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。

マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照 <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> プラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照 <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> プラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照 <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> リアルタイムデータまたは履歴データを使用したポリシー分析。ポリシーアプリケーションの事前実施の検証とリスク評価を支援し、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照 <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration->

analytics/solutionoverview-c22-739268.pdf 正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照：<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> 正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照：<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> パブリッククラウドまたはデータセンターで実行されているコンテナワークロード。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照：<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> パブリッククラウドまたはデータセンターで実行されているコンテナワークロード。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続け、アプリケーションの動作の変化に応じてセグメンテーションポリシーが最新であることを確認します。参照：<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf>

質問: 36

組織が複数のCiscoFTDアプライアンスを導入し、1つの集中型ソリューションを使用してそれらを管理したい組織にはローカルVMはありませんが、CiscoFTDに移行する必要がある既存のCiscoASAがあります。組織のニーズを満たすソリューションはどれですか。

- A. Cisco FDM
- B. CDO
- C. Cisco FMC
- D. CSM

正解: D ([コメントを发表する](#))

質問: 37

VPN機能を左から右の説明にドラッグアンドドロップします。



正解:



質問: 38

監視エージェントがパケット損失とジッター情報を収集して出力するために使用するメトリックはどれですか。

- A. RTPパフォーマンス
- B. AVCパフォーマンス
- C. OTCPのパフォーマンス
- D. WSAvのパフォーマンス

正解: B ([コメントを发表する](#))

質問: 39

組織は、クラウド環境でデータを保護したいと考えています。そのセキュリティモデルでは、すべてのユーザーが認証および承認される必要があります。アプリケーションとデータへのアクセスを許可または維持する前に、セキュリティの構成とポスチャを継続的に検証する必要があります。また、特定のアプリケーショントラフィックを許可し、デフォルトで他のすべてのトラフィックを拒否する必要があります。これらの要件を実装するには、どのテクノロジーを使用する必要がありますか？

- A. 仮想ルーティングと転送
- B. マイクロセグメンテーション
- C. アクセス制御ポリシー
- D. 仮想LAN

正解: ([正解を表示します](#))

説明

ゼロトラストは、組織のネットワークの内外を問わず、すべてのユーザーが、アプリケーションやデータへのアクセスを許可または維持する前に、セキュリティ構成とポスチャについて認証、承認、および継続的に検証されることを要求するセキュリティフレームワークです。ゼロトラストは、従来のネットワークエッジがないことを前提としています。ネットワークは、ローカル、クラウド、または任意の場所のリソースとの組み合わせまたはハイブリッド、および任意の場所のワーカーにすることができます。

ゼロトラストモデルは、マイクロセグメンテーション ネットワークのすべての部分への個別のアクセスを維持するために境界を小さなゾーンに分割することを含むセキュリティ技術)を使用して、攻撃を封じ込めます。

質問: 40

セキュリティアプリケーションがソフトウェア定義のネットワークアーキテクチャ内のコントローラに特定のセキュリティの脅威について通知するときに使用されているAPIのタイプはどれですか。 2つ選択してください)

- A. ノースバウンドAPI
- B. イーストバウンドAPI
- C. サウスバウンドAPI
- D. 西行きAP

正解: ([正解を表示します](#))

質問: 41

GETVPNとIPsecの違いは何ですか？

- A. GETVPNはIKEv2に基づいており、IKEv1をサポートしていません
- B. GETVPNは、すべてのデバイスを静的に構成することなく、複数のサイトでVPNネットワークを構築するために使用されます
- C. GETVPNは、キー管理とセキュリティアソシエーション管理を提供します
- D. GETVPNは遅延を減らし、中央ハブを使用せずにMPLSを介した暗号化を提供します

正解: ([正解を表示します](#))

質問: 42

コンテキストディレクトリエージェントの機能は何ですか？

- A. Active Directoryログを読み取り、IPアドレスをユーザー名にマップします
- B. ユーザーのグループメンバーシップを維持します
- C. WebセキュリティアプライアンスからActiveDirectoryにユーザー認証要求を中継します
- D. ユーザー識別のためにWebセキュリティアプライアンスに代わってユーザー認証要求を受け入れます

正解: ([正解を表示します](#))

質問: 43

VPNのセキュアハッシュアルゴリズムによって何が提供されますか？

- A. 整合性
- B. 鍵交換
- C. 認証
- D. 暗号化

正解: ([正解を表示します](#))

質問: 44

顧客は、イントラネットエクストラネットやインターネットなどのさまざまな外部HTTPリソースを利用でき、プロキシ構成は明示モードで実行されます。直接接続するタイミングとプロキシを使用するタイミングを選択するようにクライアントデスクトップブラウザを構成できる方法はどれですか。

- A. トランスポートモード
- B. 転送ファイル
- C. PACファイル
- D. ブリッジモード

正解: A ([コメントを發表する](#))

質問: 45

ソフトウェア定義のネットワークアーキテクチャ内のコントローラーがネットワーク内のスイッチの構成を動的に変更する場合、どのタイプのAPIが使用されますか？

- A. 西行きAP
- B. サウスバウンドAPI
- C. ノースバウンドAPI
- D. イーストバウンドAPI

正解: ([正解を表示します](#))

サウスバウンドAPIを使用すると、SDNコントローラーはリアルタイムの要求とスケーラビリティのニーズに基づいて動的に変更を加えることができます。



質問: 46

Cisco DNA Centerは、ネットワークを完全に制御するためにどのタイプのダッシュボードを提供しますか？

- A. サービス管理
- B. 集中管理
- C. アプリケーション管理
- D. 分散管理

正解: B ([コメントを发表する](#))

シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。

シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。

参照：

シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

Easy ConnectをCiscoTrustSecと併用した場合、ネットワークアクセスの制御に役立つ2つの方法はどれですか。(2つ選択してください)

- A. 複数のセキュリティ製品が情報を共有し、連携してネットワークのセキュリティ体制を強化できるようにします。

- B. 接続されているすべてのエンドポイントの完全な可視性を提供するダッシュボードをCiscoISEに作成します。
- C. セキュリティグループタグの割り当てが可能であり、スイッチまたはエンドポイントで802.1xを設定する必要はありません。
- D. サードパーティ製品と統合して、ネットワーク全体の可視性を向上させます。
- E. ADに対して認証される管理対象エンドポイントをセキュリティグループ (PassiveID)にマッピングできます。

正解: ([正解を表示します](#))

Easy Connectは、有線接続または無線接続のどちらを使用する場合でも、エンドポイントで802.1Xを必要とせずに、セキュリティグループタグをエンドポイントに割り当てることができるため、ネットワークアクセスの制御とセグメンテーションを簡素化します。参照：

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf>802.1Xを必要とせずにエンドポイントにタグをグループ化有線接続か無線接続かに関係なく、これらのエンドポイント。

Easy Connectは、有線接続または無線接続のどちらを使用する場合でも、エンドポイントで802.1Xを必要とせずに、セキュリティグループタグをエンドポイントに割り当てることができるため、ネットワークアクセスの制御とセグメンテーションを簡素化します。参照：

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf>

質問: 48

管理者ログインが機能するためにCiscoISEでシャドウユーザを作成する必要があるIDストアはどれですか。

- A. 内部データベース
- B. LDAP
- C. Active Directory
- D. RSA SecureID

正解: C ([コメントを發表する](#))

質問: 49

ストリームを使用して運用データをプッシュし、アクティビティのほぼリアルタイムのビューを提供するネットワーク監視ソリューションはどれですか？

- A. SNMP
- B. SMTP
- C. syslog
- D. モデル駆動型テレメトリ

正解: ([正解を表示します](#))

プルモデルの従来の使用法では、クライアントがネットワークにデータを要求しますが、必要なものがリアルタイムデータに近い場合はスケーリングされません。さらに、一部のユースケースでは、インターフェイスステータス、プロトコルネイバーの変更など、一部のデータが変更された場合にのみ通知する必要があります。

モデル駆動型テレメトリは、プッシュモデルを使用してネットワークデバイスからデータが継続的にストリーミングされ、運用統計へのほぼリアルタイムのアクセスを提供する、ネットワーク監視の新しいアプローチです。

アプリケーションは、NETCONF-YANGを介して標準ベースのYANGデータモデルを使用することにより、必要な特定のデータ項目をサブスクライブできます。Cisco IOS XEストリーミングテレメトリを使用すると、データをデバイスから外部コレクタに、はるかに高い周波数で、より効率的にプッシュできます。また、データオンチェンジストリーミングも可能です。

プルモデルの従来の使用法では、クライアントがネットワークにデータを要求しますが、必要なものがリアルタイムデータに近い場合はスケーリングされません。さらに、一部のユースケースでは、インターフェイスステータス、プロトコルネイバーの変更など、一部のデータが変更された場合にのみ通知する必要があります。

モデル駆動型テレメトリは、プッシュモデルを使用してネットワークデバイスからデータが継続的にストリーミングされ、運用統計へのほぼリアルタイムのアクセスを提供する、ネットワーク監視の新しいアプローチです。

アプリケーションは、NETCONF-YANGを介して標準ベースのYANGデータモデルを使用することにより、必要な特定のデータ項目をサブスクライブできます。Cisco IOS XEストリーミングテレメトリを使用すると、データをデバイスから外部コレクタに、はるかに高い周波数で、より効率的にプッシュできます。また、データオンチェンジストリーミングも可能です。

プルモデルの従来の使用法では、クライアントがネットワークにデータを要求しますが、必要なものがリアルタイムデータに近い場合はスケーリングされません。さらに、一部のユースケースでは、インターフェイスステータス、プロトコルネイバーの変更など、一部のデータが変更された場合にのみ通知する必要があります。

モデル駆動型テレメトリは、プッシュモデルを使用してネットワークデバイスからデータが継続的にストリーミングされ、運用統計へのほぼリアルタイムのアクセスを提供する、ネットワーク監視の新しいアプローチです。

アプリケーションは、NETCONF-YANGを介して標準ベースのYANGデータモデルを使用することにより、必要な特定のデータ項目をサブスクライブできます。Cisco IOS XEストリーミングテレメトリを使用すると、データをデバイスから外部コレクタに、はるかに高い周波数で、より効率的にプッシュできます。また、データオンチェンジストリーミングも可能です。

質問: 50

エンジニアは、プロトコルフィールドを分析し、産業用システムからのトラフィックの異常を検出するようにCiscoFTDを設定する任務を負っています。これらの要件を満たすために何をしなければなりませんか？

- A. CIPプリプロセッサのプレフィルタポリシーを実装する
- B. CiscoFTDでトラフィック分析を有効にします
- C. DNP3プリプロセッサの侵入ルールを設定します
- D. 産業用トラフィックを信頼するようにアクセス制御ポリシーを変更します

正解: ([正解を表示します](#))

Modbus、DNP3、およびCIP SCADAプリプロセッサは、トラフィックの異常を検出し、侵入ルールにデータを提供します。したがって、この質問では、回答Aまたは回答Cのみが正しいです。DNP3プリプロセッサは、DNP3トラフィックの異常を検出し、DNP3キーワードを使用して特定のプロトコルフィールドにアクセスするルールエンジンで処理するためにDNP3プロトコルをデコードします。共通産業プロトコル (CIP)は、産業自動化アプリケーションをサポートする広く使用されているアプリケーションプロトコルです。EtherNet / IPは、イーサネットベースのネットワークで使用されるCIPの実装です。CIPプリプロセッサは、TCPまたはUDPで実行されているCIPおよびENIPトラフィックを検出し、侵入ルールエンジンに送信します。カスタム侵入ルールでCIPおよびENIPキーワードを使用して、CIPおよびENIPトラフィックの攻撃を検出できます。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-configguide-v63/scada_preprocessors.html DNP3プリプロセッサとCIPプリプロセッサの両方を使用してトラフィックの異常を検出できますが、CIPをそのまま選択します産業用アプリケーションで広く使用されています。注 :+侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。html DNP3とCIPの両方のプリプロセッサを使用してトラフィックの異常を検出できますが、産業用アプリケーションで広く使用されているため、CIPを選択します。注 :+侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。html DNP3とCIPの両方のプリプロセッサを使用し

てトラフィックの異常を検出できますが、産業用アプリケーションで広く使用されているため、CIPを選択します。注 +侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。+侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。+侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。これは、ネットワーク分析ポリシーのプリプロセッサとパケットデコーダの検出オプションに関連するルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。これは、ネットワーク分析ポリシーのプリプロセッサとパケットデコーダの検出オプションに関連するルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。

ルール。したがって、この質問では、回答Aまたは回答Cのみが正しいです。

DNP3プリプロセッサは、DNP3トラフィックの異常を検出し、DNP3キーワードを使用して特定のプロトコルフィールドにアクセスするルールエンジンで処理するためにDNP3プロトコルをデコードします。

共通産業プロトコル (CIP)は、産業自動化アプリケーションをサポートする広く使用されているアプリケーションプロトコルです。EtherNet / IPは、イーサネットベースのネットワークで使用されるCIPの実装です。CIPプリプロセッサは、TCPまたはUDPで実行されているCIPおよびENIPトラフィックを検出し、侵入ルールエンジンに送信します。

カスタム侵入ルールでCIPおよびENIPキーワードを使用して、CIPおよびENIPトラフィックの攻撃を検出できます。

参照：

DNP3とCIPの両方のプリプロセッサを使用してトラフィックの異常を検出できますが、産業用アプリケーションで広く使用されているため、CIPを選択します。

ノート：

Modbus、DNP3、およびCIP SCADAプリプロセッサは、トラフィックの異常を検出し、侵入ルールにデータを提供します。したがって、この質問では、回答Aまたは回答Cのみが正しいです。DNP3プリプロセッサは、DNP3トラフィックの異常を検出し、DNP3キーワードを使用して特定のプロトコルフィールドにアクセスするルールエンジンで処理するためにDNP3プロトコルをデコードします。共通産業プロトコル (CIP)は、産業自動化アプリケーションをサポートする広く使用されているアプリケーションプロトコルです。EtherNet / IPは、イーサネットベースのネットワークで使用されるCIPの実装です。CIPプリプロセッサは、TCPまたはUDPで実行されているCIPおよびENIPトラフィックを検出し、侵入ルールエンジンに送信します。カスタム侵入ルールでCIPおよびENIPキーワードを使用して、CIPおよびENIPトラフィックの攻撃を検出できます。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-configguide-v63/scada_preprocessors.html DNP3プリプロセッサとCIPプリプロセッサの両方を使用してトラフィックの異常を検出できますが、CIPをそのまま選択します産業用アプリケーションで広く使用されています。注 +侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。html DNP3とCIPの両方のプリプロセッサを使用してトラフィックの異常を検出できますが、産業用アプリケーションで広く使用されているため、CIPを選択します。注 +侵入ルールは、ネッ

トワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。html DNP3とCIPの両方のプリプロセッサを使用してトラフィックの異常を検出できますが、産業用アプリケーションで広く使用されているため、CIPを選択します。注 +侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。+侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。+侵入ルールは、ネットワークの脆弱性を悪用する試みを検出するためにシステムが使用する、指定された一連のキーワードと引数です。システムはネットワークトラフィックを分析するときに、パケットを各ルールで指定された条件と比較し、データパケットがルールで指定されたすべての条件を満たしている場合にルールをトリガーします。+プリプロセッサルール。これは、ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられたルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。これは、ネットワーク分析ポリシーのプリプロセッサとパケットデコーダの検出オプションに関連するルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。これは、ネットワーク分析ポリシーのプリプロセッサとパケットデコーダの検出オプションに関連するルールです。ほとんどのプリプロセッサルールはデフォルトで無効になっています。

質問: 51

NetFlowエクスポートフォーマットを左から右の説明にドラッグアンドドロップします。

Version 1	appropriate only for the main cache
Version 5	introduced support for aggregation caches
Version 8	appropriate only for legacy systems
Version 9	introduced extensibility

正解:



Explanation:バージョン1フォーマットは、最初にリリースされたバージョンでした。バージョン1を必要とするレガシー収集システムを使用している場合を除き、バージョン1形式は使用しないでください。バージョン9またはバージョン5のエクスポート形式を使用します。バージョン5のエクスポート形式は、メインキャッシュにのみ適しています。新しい機能をサポートするために拡張することはできません。バージョン8のエクスポート形式は、集約キャッシュでのみ使用できます。新しい機能をサポートするために拡張することはできません。参照 <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgnflow-data-expt.html>

質問: 52

Cisco Workload Optimization Managerは、アプリケーションのパフォーマンスの問題を軽減するのにどのように役立ちますか。

- A. AWS Lambdaシステムをデプロイします
- B. リソースのサイズ変更を自動化します
- C. 流路を最適化します
- D. ワークロードフォレンジックスコアを設定します

正解: (正解を表示します)

Cisco Workload Optimization Managerは、ワークロードが必要なときに必要なリソースを確実に取得できるようにする特定のリアルタイムアクションを提供し、自動化できる継続的な配置、サイズ変更、および容量の決定を可能にして、環境の継続的な正常性を促進します。快適さのレベルに応じて、ソフトウェアの決定を自動化できます。推奨（表示のみ）、手動（選択して適用）、または自動化（ソフトウェアによってリアルタイムで実行）。参照：
<https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf>必要なときに必要なリソース、自動化できる継続的な配置、サイズ変更、および容量の決定を可能にし、環境の継続的な健全性を促進します。快適さのレベルに応じて、ソフトウェアの決定を自動化できます。

Cisco Workload Optimization Managerは、ワークロードが必要なときに必要なリソースを確実に取得できるようにする特定のリアルタイムアクションを提供し、自動化できる継続的な配置、サイズ変更、および容量の決定を可能にして、環境の継続的な正常性を促進します。快適さのレベルに応じて、ソフトウェアの決定を自動化できます。推奨（表示のみ）、手動（選択して適用）、または自動化（ソフトウェアによってリアルタイムで実行）。参照：
<https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf>

質問: 53

構成されたポスチャポリシー要件が満たされていない場合、どのコンプライアンスステータスが表示されますか？

- A. 非準拠
- B. 承認済み
- C. 準拠
- D. 不明

正解: **A** ([コメントを发表する](#))

質問: **54**

ユーザーがオンプレミスのESAソリューションとCESソリューションを選択するのはなぜですか？

- A. サーバーチームはこのサービスを外部委託したいと考えています。
- B. 需要は予測できません。
- C. ESAはインラインで展開されます。
- D. 機密データはオンサイトに残しておく必要があります。

正解: **D** ([コメントを发表する](#))

質問: **55**

Cisco ISEをMDMソリューションと統合する利点は何ですか？

- A. ネットワークへのアクセスのコンプライアンスチェックを提供します
- B. モバイルデバイス上の他のアプリケーションを更新する機能を提供します
- C. Cisco ISEを介してモバイルデバイスにアプリケーションを追加する機能を提供します
- D. ネットワークデバイス管理アクセスを提供します

正解: **A** ([コメントを发表する](#))

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

質問: **56**

デバイスコンプライアンスチェックを実施する利点は何ですか？

- A. A
- B. B

正解: ([正解を表示します](#))



質問: **57**

PKIでのCAの目的は何ですか？

- A. デジタル証明書を発行および取り消す
- B. デジタル証明書の信頼性を検証する
- C. デジタル証明書の秘密鍵を作成するには
- D. 指定されたサブジェクトによる公開鍵の所有権を証明するため

正解: ([正解を表示します](#))

説明信頼できるCAは、信頼できるデジタル証明書を発行できる唯一のエンティティです。PKIはこれらの証明書の暗号化側の多くを管理しますが、認証はどのエンティティがどのキーを所有しているかを理解するために不可欠であるため、これは非常に重要です。信頼できるCAがなければ、誰でも自分のキーを発行でき、認証はウィンドウの外に出て、混乱が生じます。参照 <https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/>信頼できるCAは、信頼できるデジタル証明書を発行できる唯一のエンティティです。PKIはこれらの証明書の暗号化側の多くを管理しますが、認証はどのエンティティがどのキーを所有しているかを理解するために不可欠であるため、これは非常に重要です。信頼できるCAがなければ、誰でも自分のキーを発行でき、認証はウィンドウの外に出て、混乱が生じます。参照 <https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/>

質問: 58

Cisco DNA Centerは、ネットワークを完全に制御するためにどのタイプのダッシュボードを提供しますか？

- A. サービス管理
- B. 集中管理
- C. アプリケーション管理
- D. 分散管理

正解: [\(正解を表示します\)](#)

シスコのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。参照: <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-faq-cte-en.html> CiscoのDNAセンターは、このすべての機能を1つのガラス板にまとめた唯一の集中型ネットワーク管理システムです。参照 <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-faq-cte-en.html>

質問: 59

VPNの展開を計画するとき、エンジニアはDMVPNではなくアクティブ/アクティブFlexVPN構成を選択する理由は何ですか？

- A. HSRPはfalioverに使用されます。
- B. フローティング静的ルートが必要です。
- C. 複数のルーターまたはVRFが必要です。
- D. トラフィックはデフォルトで静的に分散されます。

正解: D ([コメントを發表する](#))

質問: 60

パケットTTL、IP/TCPフラグ、ペイロード長など、フロー内で見られる変動をキャプチャするテレメトリデータはどれですか？

- A. プロセス詳細のバリエーション
- B. ソフトウェアパッケージのバリエーション
- C. フローインサイトのバリエーション
- D. パケット間バリエーション

正解: D ([コメントを發表する](#))

質問: 61

マネージドIntercloudFabricデプロイメントモデルの2つのタイプは何ですか？ 2つ選択してください。）

- A. パブリックマネージド
- B. サービスプロバイダーが管理
- C. エンタープライズ管理
- D. ユーザー管理
- E. ハイブリッドマネージド

正解: ([正解を表示します](#))

The Cisco Intercloud Fabric architecture provides two product configurations to address the following two consumption models:

- Cisco Intercloud Fabric for Business
- Cisco Intercloud Fabric for Providers



有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **62**

CiscoASA用のCiscoNetFlowセキュアイベントロギングの機能は何ですか。

- A. 複数のNetFlowコレクターがサポートされています。
- B. 高度なNetFlowv9テンプレートとレガシーv5フォーマットがサポートされています。
- C. フロー作成イベントが遅延します。
- D. セキュアNetFlow接続はCiscoPrimeInfrastructure用に最適化されています

正解: ([正解を表示します](#))

参照 :

Each NSEL data record has the event time field (NF_F_EVENT_TIME_MSEC), which is the time that the event occurred in milliseconds. The NetFlow packet may consist of multiple events; however, the time that the packet is sent does not represent the time that the event occurred, because the NetFlow service waits for multiple events to pack the NetFlow packet.

質問: **63**

組織がCiscoFTDまたはCiscoASAデバイスを使用したい特定のURLがファイアウォールを介してアクセスされないようにブロックする必要があるため、管理者は、組織がブロックしたい不正なURLカテゴリをアクセスポリシーに入力する必要があります。この要件を満たすには、どのソリューションを使用する必要がありますか。？

- A. rtはデフォルトでURLフィルタリングを有効にし、悪意のあるURLをブロックするのにに対し、Cisco ASAはそうではないため、Cisco FTD
- B. アクセスコントロールポリシー機能にURLフィルタリングが含まれているのにに対し、CiscoASAには含まれていないためのCiscoFTD。
- C. Cisco ASAは、デフォルトでURLフィルタリングを有効にし、悪意のあるURLをブロックしますが、CiscoFTDはブロックしません。
- D. Cisco ASAは、アクセスコントロールポリシー機能にURLフィルタリングが含まれているのにに対し、CiscoFTDには含まれていないためです。

正解: **A** ([コメントを发表する](#))

質問: **64**

エンジニアは、ネットワーク内のCiscoスイッチで802.1X認証を設定し、メカニズムとしてCoAを使用しています。CoAトラフィックがネットワークを通過できるようにするには、ファイアウォールのどのポートを開く必要がありますか？

- A. TCP 6514
- B. UDP 1700
- C. TCP 49
- D. UDP 1812

正解: B (コメントを发表する)

- RADIUS Change of Authorization (CoA) Send: UDP/1700
- RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799

質問: 65

組織がCiscoFTDまたはCiscoASAデバイスを使用したいと考えています。特定のURLがファイアウォールを介してアクセスされるのをブロックする必要があります。これにより、管理者は、組織がブロックしたい不正なURLカテゴリをアクセスポリシーに入力する必要があります。この要件を満たすには、どのソリューションを使用する必要がありますか？

- A. Cisco ASAは、デフォルトでURLフィルタリングを有効にし、悪意のあるURLをブロックしますが、CiscoFTDはブロックしません。
- B. アクセス制御ポリシー機能にURLフィルタリングが含まれているのに対し、CiscoASAには含まれていないCiscoFTD
- C. Cisco FTDは、デフォルトでURLフィルタリングを有効にし、悪意のあるURLをブロックしますが、CiscoASAはブロックしません。
- D. アクセス制御ポリシー機能にURLフィルタリングが含まれているため、Cisco ASAが含まれていますが、CiscoFTDには含まれていません。

正解: (正解を表示します)

質問: 66

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

superior threat prevention and mitigation for known and unknown threats

superior threat prevention and mitigation for known and unknown threats

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

説明

superior threat prevention and mitigation for known and unknown threats

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

質問: 67

VPN機能を左から右の説明にドラッグアンドドロップします。

IPsec

AES

SHA-1

ISAKMP

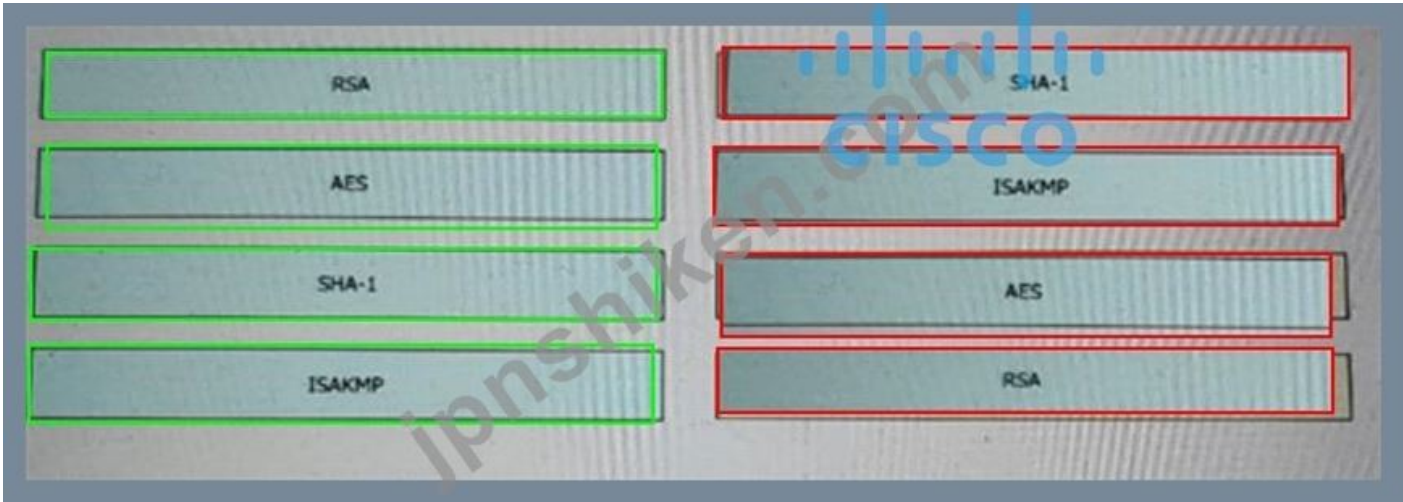
ensures data integrity

defines IKE SAs

ensures data confidentiality

provides authentication

正解:



質問: 68

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

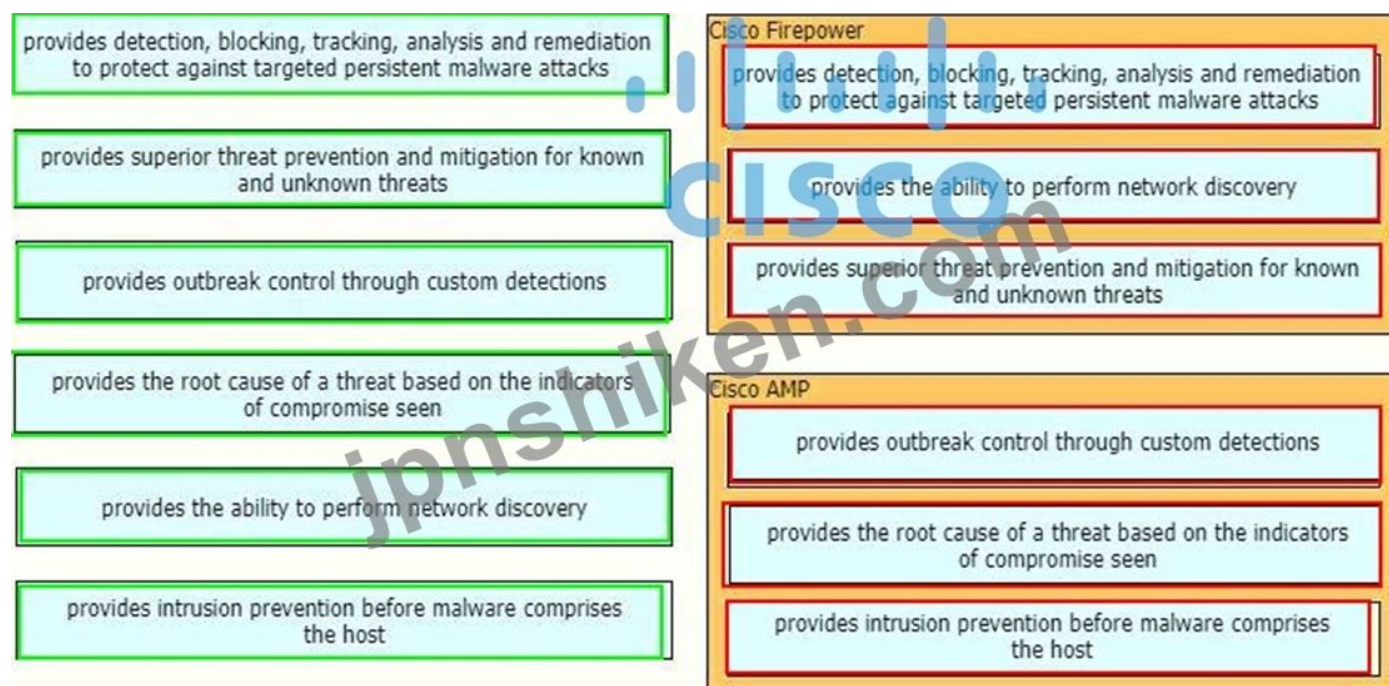
provides the ability to perform network discovery

provides intrusion prevention before malware compromises the host

Cisco Firepower

Cisco AMP

正解:



質問: 69

Ciscoスイッチで802.1Xをグローバルに有効にするコマンドはどれですか。

- A. 認証ポート制御aut
- B. dot1xpaeオーセンティケーター
- C. dot1x system-auth-control
- D. aaa new-model

正解: C ([コメントを发表する](#))

質問: 70

ネットワーク管理者は、802.1X用のCisco ISEを使用するようにスイッチを設定しています。エンドポイントが認証に失敗しており、ネットワークにアクセスできません。管理者は、認証の詳細を確認するためにどこからトラブルシューティングを開始する必要がありますか？

- A. 適応型ネットワーク制御ポリシーリスト
- B. コンテキストの可視性
- C. 会計報告
- D. RADIUSライブログ

正解: D ([コメントを发表する](#))

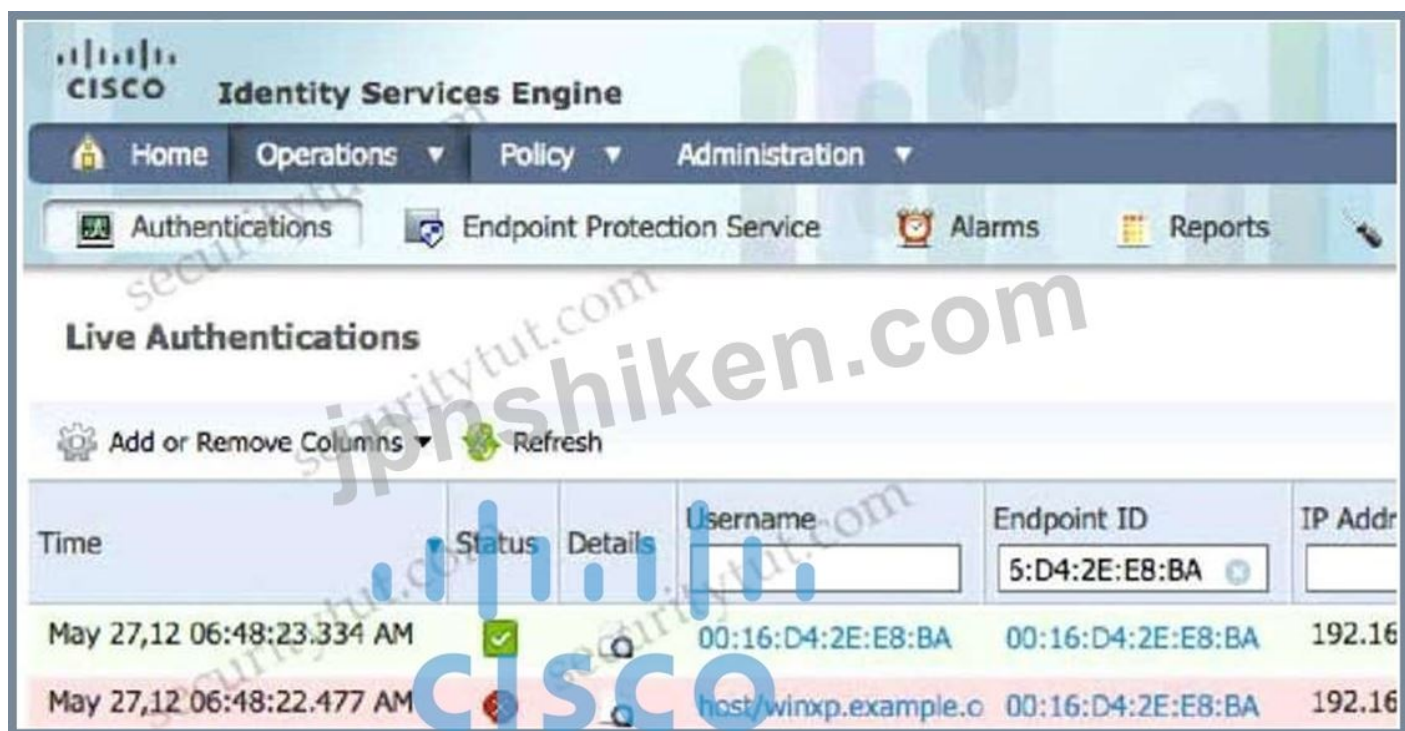
ISEで失敗した認証と許可のトラブルシューティング方法のトラブルシューティング方法

ISEライブログを確認してください

プライマリISEポリシー管理ノード (PAN)にログインします。

[操作]>[RADIUS]>[ライブログ]に移動します

オプション) イベントがRADIUSライブログに存在しない場合は、[操作]>[レポート]>[レポート]>[エンドポイントとユーザー]>[RADIUS認証]に移動し、ログで失敗した認証試行を確認します



質問: 71

MFAはどのタイプの攻撃に対して効果的な抑止力ですか？

- A. シンフラッド
- B. ping of death
- C. フィッシング
- D. ティアドロップ

正解: ([正解を表示します](#))

質問: 72

展示を参照してください。



管理者が新しいCiscoFTDデバイスをネットワークに追加していて、CiscoFMCで管理したいと考えています。CiscoFTDはNATデバイスの背後にありません。Cisco FTDでこれを有効にするには、どのコマンドが必要ですか。

- A. マネージャーを構成してDONTRESOLVE登録キーを追加>
- B. configure manager add <FMC IP address> <registration key> 16

- C. configure manager addDONTRESOLVE<登録キー>FTD123
D. configure manager add <FMC IP address> <registration key>

正解: (正解を表示します)

FMCにFTDを管理させるには、まずFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド `configuremanageradd 1.1.1.2 the_registration_key_you_want 1.1.1.2`(1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。参照 <https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/choice>。コマンド `configuremanageradd 1.1.1.2 the_registration_key_you_want 1.1.1.2`(1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。

FMCにFTDを管理させるには、まずFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド `configuremanageradd 1.1.1.2 the_registration_key_you_want 1.1.1.2`(1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。参照 <https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/>

質問: 73

展示を参照してください。

```
*Jun 30 16:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP:(1001):purging SA., sa=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5; retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.299: ISAKMP:(1002):peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

ネットワーク管理者が2つのCiscoIOSルータ間にサイト間VPNトンネルを設定したため、ホストはVPNの2つのサイト間で通信できません。ネットワーク管理者は、`debug crypto isakmp sa`コマンドを実行して、VPNステータスを追跡します。このコマンド出力による問題は何ですか。

- A. ハッシュアルゴリズムの不一致
B. 興味深いトラフィックは適用されませんでした
C. 暗号化アルゴリズムの不一致

D. 認証キーの不一致
正解: [\(正解を表示します\)](#)

質問: 74

一般的なセキュリティの脅威を左から右の定義にドラッグアンドドロップします。

phishing	a software program that copies itself from one computer to another, without human interaction
botnet	unwanted messages in an email inbox
spam	group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse
worm	fraudulent attempts by cyber criminals to obtain private information

正解:

phishing	worm
botnet	spam
spam	botnet
worm	phishing

質問: 75

Cisco Firepower Next Generation Intrusion Prevention Systemのホスト情報をキャプチャするために使用されるポリシーはどれですか？

- A. 相関
- B. 侵入
- C. アクセス制御
- D. ネットワークディスカバリー

正解: D [\(コメントを发表する\)](#)

Firepowerシステムは、ネットワーク検出およびIDポリシーを使用して、ネットワーク上のトラフィックのホスト、アプリケーション、およびユーザーデータを収集します。特定の種類の検出およびIDデータを使用して、ネットワーク資産の包括的なマップを構築し、フォレンジック分析、動作プロファイリング、アクセス制御を実行し、組織が影響を受けやすい脆弱性とエクスプロイトを軽減および対応できます。ホストとアプリケーションの検出を実行するようにネットワーク検出ポリシーを構成できます。参照 :ネットワーク上のトラフィックについては、https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.htmlを参照してください。特定の種類の検出およびIDデータを使用して、ネットワーク資産の包括的なマップを作成し、フォレンジック分析を実行し、ホストとアプリケーションの検出を実行するようにネットワーク検出ポリシーを構成できます。

Firepowerシステムは、ネットワーク検出およびIDポリシーを使用して、ネットワーク上のトラフィックのホスト、アプリケーション、およびユーザーデータを収集します。特定の種類の検出およびIDデータを使用して、ネットワーク資産の包括的なマップを構築し、フォレンジック分析、動作プロファイリング、アクセス制御を実行し、組織が影響を受けやすい脆弱性とエクスプロイトを軽減および対応できます。ホストとアプリケーションの検出を実行するようにネットワーク検出ポリシーを構成できます。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html

質問: 76

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

正解:

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

uses six packets in main mode to establish phase 1

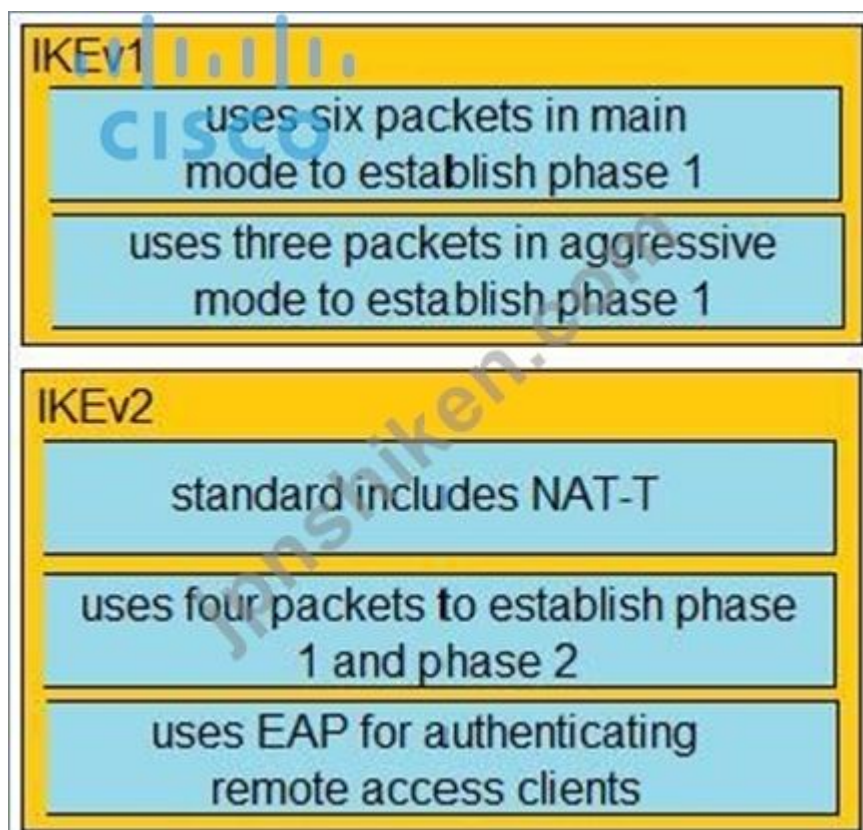
uses three packets in aggressive mode to establish phase 1

IKEv2

standard includes NAT-T

uses four packets to establish phase 1 and phase 2

uses EAP for authenticating remote access clients



有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> 727問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 77

AWSパブリッククラウド内にCiscoASAvをデプロイするときにサポートされる機能はどれですか。

- A. マルチコンテキストモード
- B. レイヤー3ネットワークのユーザー展開
- C. IPv6
- D. クラスタリング

正解: ([正解を表示します](#))

説明/リファレンス <https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav-aws.html>

質問: 78

エンドポイントに一貫してパッチを適用することが重要なのはなぜですか？

- A. ベンダー契約ごとにパッチが必要です。
- B. パッチは脆弱性を軽減するのに役立ちます。
- C. パッチを適用すると、インフラストラクチャの攻撃対象領域が減少します。
- D. パッチを適用すると、ハニーポットを作成できます。

正解: B ([コメントを发表する](#))

質問: 79

展示を参照してください。

```
snmp-server group SNMP v3 auth access 15
```

この構成では、15という数字は何を表していますか？

- A. このルーターに対する許可されたユーザーの特権レベル
- B. ルーターにアクセスできるSNMPデバイスを識別するアクセスリスト
- C. SNMPv3認証の試行間の秒単位の間隔
- D. SNMPv3ユーザーがロックアウトされるまでに失敗した可能性のある試行の数

正解: ([正解を表示します](#))

質問: 80

```
SwitchA (config)# interface gigabitethernet1/0/1
SwitchA (config-if)# dot1x host-mode multi-host
SwitchA (config-if)# dot1x timeout quiet-period 3
SwitchA (config-if)# dot1x timeout tx-period 15
SwitchA (config-if)# authentication port-control auto
SwitchA (config-if)# switchport mode access
SwitchA (config-if)# switchport access vlan 12
```

展示を参照してください。エンジニアがネットワーク上に有線802.1xを設定しましたが、ラップトップを認証することができません。どのポート構成が欠落していますか？

- A. dot1x再認証
- B. cisp enable
- C. dot1xpaeオーセンティケーター
- D. 認証オープン

正解: ([正解を表示します](#))

説明/参照 :

質問: 81

組織は、短期間に大量のスパムメッセージを受信しました。メッセージに対してアクションを実行するには、メッセージがどれほど有害であるかを判断する必要があります、これは動的に発生する必要があります。これを実現するには何を構成する必要がありますか？

- A. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoWSAを設定します。
- B. Talosからリアルタイムアップデートを受信するようにCiscoESAを設定します
- C. Talosからリアルタイムアップデートを受信するようにCiscoWSAを設定します。
- D. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoESAを設定します。

正解: ([正解を表示します](#))

https://www.cisco.com/c/en/us/td/docs/security/esa/esa120/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01100.html

質問: 82

死の攻撃のpingを特徴付ける2つの行動パターンはどれですか？ (2つ選択してください。)

- A. 攻撃は送信前に8オクテットのグループに断片化されます。
- B. 攻撃は、送信前に16オクテットのグループに断片化されます。
- C. 通常、攻撃を実行するために公的にアクセス可能なDNSサーバーが使用されます。
- D. 不正な形式のパケットは、システムをクラッシュさせるために使用されます。
- E. トラフィックの短い同期バーストは、TCP接続を中断するために使用されます。

正解: ([正解を表示します](#))

質問: 83

データセキュリティのためのCiscoCloudlockの機能は何ですか？

- A. データ損失防止
- B. 悪意のあるクラウドアプリを制御します
- C. 異常を検出します
- D. ユーザーとエンティティの行動分析

正解: ([正解を表示します](#))

説明/参照 <https://umbrella.cisco.com/products/casb>

質問: 84

ネットワークエンジニアは、ネットワークに新しい医療機器を追加する任務を負っています。Cisco ISEがNACサーバとして使用されており、新しいデバイスには使用可能なサブリカントがありません。このデバイスをネットワークに安全に接続するには、何をする必要がありますか？

- A. プロファイリングでMABを使用する
- B. 姿勢評価でMABを使用します。
- C. 姿勢評価で802.1Xを使用します。
- D. プロファイリングで802.1Xを使用します。

正解: ([正解を表示します](#))

新しいデバイスにはサブリカントがないため、802.1Xを使用できません。

MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。

Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意の識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。

分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づいて、ユーザーに差別化されたネットワークアクセスを提供することです。たとえば、従業員は会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。

新しいデバイスにはサブリカントがないため、802.1Xを使用できません。

MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。

Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意的識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。

分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づいて、ユーザーに差別化されたネットワークアクセスを提供することです。たとえば、従業員は会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。新しいデバイスにはサブリカントがないため、802.1Xを使用できません。

MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。

Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意的識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。

分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づいて、ユーザーに差別化されたネットワークアクセスを提供することです。たとえば、従業員は会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。

質問: 85

NetFlowセキュアイベントロギングの機能は何ですか？

- A. RSVPを介したトラフィックとイベントタイプに基づいてNSELイベントをフィルタリングします。
- B. NetFlowoverTCPのみを介してNSELコレクターにデータレコードを配信します。
- C. フロー内の重要なイベントを示すレコードのみをエクスポートします。
- D. v5およびv8テンプレートをサポートします。

正解: ([正解を表示します](#))

質問: 86

CiscoFirepowerのセキュリティインテリジェンスポリシーを使用します。Firepowerブロックベースの2つの基準はどれですか。2つ選択してください。)

- A. プロトコルID
- B. URL
- C. IPアドレス
- D. ポート番号
- E. MACアドレス

正解: B,C ([コメントを发表する](#))



質問: 87

Firepower Next Generation Intrusion Prevention Systemで使用されている2つのアプリケーション層プリプロセッサはどれですか？ 2つ選択してください。)

- A. SIP
- B. インライン正規化
- C. SSL
- D. パケットデコーダー
- E. modbus

正解: ([正解を表示します](#))

説明/リファレンス https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html

質問: 88

最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

- A. アクセスポリシーを変更する
- B. 識別プロファイルを変更する
- C. アウトバウンドマルウェアスキャンポリシーを変更する
- D. Webプロキシ設定を変更する

正解: ([正解を表示します](#))

アクセス制御ルールのURL条件を使用すると、ネットワーク上のユーザーがアクセスできるWebサイトを制限できます。この機能はURLフィルタリングと呼ばれます。アクセス制御を使用して、ブロックする または逆に許可する)URLを指定する方法は2つあります。

-どのライセンスでも、個々のURL、URLのグループ、およびURLリストとフィードを手動で指定して、Webトラフィックをきめ細かくカスタム制御できます。

-URLフィルタリングライセンスを使用すると、URLの一般的な分類またはカテゴリ、リスクレベル、またはレピュテーションに基づいてWebサイトへのアクセスを制御することもできます。システムは、このカテゴリとレピュテーションデータを接続ログ、侵入イベント、およびアプリケーションの詳細に表示します。

カテゴリとレピュテーションデータを使用すると、ポリシーの作成と管理も簡素化されます。これにより、システムがWebトラフィックを期待どおりに制御することが保証されます。最後に、シスコの脅威インテリジェンスは、新しいURL、および既存のURLの新しいカテゴリとリスクで継続的に更新されるため、システムが最新の情報を使用して要求されたURLをフィルタリングできるようにすることができます。マルウェア、スパム、ボットネット、フィッシングなどのセキュリティの脅威を表す悪意のあるサイトは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。

参照：

-どのライセンスでも、個々のURL、URLのグループ、およびURLリストとフィードを手動で指定して、Webトラフィックをきめ細かくカスタム制御できます。

-URLフィルタリングライセンスを使用すると、URLの一般的な分類またはカテゴリ、リスクレベル、またはレピュテーションに基づいてWebサイトへのアクセスを制御することもできます。システムは、このカテゴリとレピュテーションデータを接続ログ、侵入イベント、およびアプリケーションの詳細に表示します。

カテゴリとレピュテーションデータを使用すると、ポリシーの作成と管理も簡素化されます。これにより、システムがWebトラフィックを期待どおりに制御することが保証されます。最後に、シスコの脅威インテリジェンスは、新しいURL、および既存のURLの新しいカテゴリとリスクで継続的に更新されるため、システムが最新の情報を使用して要求されたURLをフィルタリングできるようにすることができます。マルウェア、スパム、ボットネット、フィッシングなどのセキュリティの脅威を表す悪意のあるサイトは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。

アクセス制御ルールのURL条件を使用すると、ネットワーク上のユーザーがアクセスできるWebサイトを制限できます。この機能はURLフィルタリングと呼ばれます。アクセス制御を使用して、ブロックする または逆に許可する)URLを指定する方法は2つあります。

-どのライセンスでも、個々のURL、URLのグループ、およびURLリストとフィードを手動で指定して、Webトラフィックをきめ細かくカスタム制御できます。

-URLフィルタリングライセンスを使用すると、URLの一般的な分類またはカテゴリ、リスクレベル、またはレピュテーションに基づいてWebサイトへのアクセスを制御することもできます。システムは、このカテゴリとレピュテーションデータを接続ログ、侵入イベント、およびアプリケーションの詳細に表示します。

カテゴリとレピュテーションデータを使用すると、ポリシーの作成と管理も簡素化されます。これにより、システムがWebトラフィックを期待どおりに制御することが保証されます。最後に、シスコの脅威インテリジェンスは、新しいURL、および既存のURLの新しいカテゴリとリスクで継続的に更新されるため、システムが最新の情報を使用して要求されたURLをフィルタリングできるようにすることができます。マルウェア、スパム、ボットネット、フィッシングなどのセキュリティの脅威を表す悪意のあるサイトは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。

質問: **89**

展示を参照してください。

```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
```

展示を参照してください。Cisco ISE管理者は、802.1X展開に新しいスイッチを追加し、一部のエンドポイントがアクセスを取得するのに問題があります。

ほとんどのPCとIP電話は、マシン証明書の資格情報を使用して接続および認証できます。ただし、プリンタとビデオカメラは提供されたインターフェイス設定に基づくことはできません。セキュリティ制御を維持しながら、認証と許可のためにCisco ISEを使用してこれらのデバイスをネットワークに接続するにはどうすればよいですか。

- A. インターフェース構成にmabを追加します。
- B. 認証イベントの設定失敗再試行2アクションインターフェイスでVLAN41を許可します
- C. Cisco ISEのデフォルトポリシーを変更して、マシン認証を使用しないすべてのデバイスを許可します。
- D. 許可されたプロトコル設定でCisco ISE内の安全でないプロトコルを有効にします。

正解: ([正解を表示します](#))

質問: 90

16進表現などの代替エンコーディングが最も頻繁に観察される攻撃の形式はどれですか？

- A. スマーフ
- B. 分散型サービス拒否
- C. クロスサイトスクリプティング
- D. ルートキット 익스プロイト

正解: ([正解を表示します](#))

クロスサイトスクリプティング (XSSとも呼ばれます)は、Webアプリケーションがユーザーから悪意のあるデータを収集するときに発生します。データは通常、悪意のあるコンテンツを含むハイパーリンクの形式で収集されます。ユーザーは、別のWebサイト、インスタントメッセージ、または単にWebボードや電子メールメッセージを読んでいるときに、このリンクをクリックする可能性があります。

通常、攻撃者はサイトへのリンクの悪意のある部分をHEX (または他のエンコード方法)でエンコードするため、クリックされたときに要求がユーザーに見えることはそれほど疑わしくありません。

たとえば、以下のコードは16進数で記述されています。<a

href = javascript :alert(

'x28'XSS')>ここをクリック

と同等です：

<ahref=javascript:alert('XSS')>ここをクリック

注：&#xhhhh」の形式では、hhhhは16進形式のコードポイントです。

質問: 91

エンドポイントがゲストアクセスと共有されるプロビジョニングWLANに関連付けられており、同じゲストポータルがBYODポータルとして使用されている場合の用語は何ですか。

A. デュアルSSID BYOD

B. マルチチャネルGUI

C. シングルSSID BYOD

D. 合理化されたアクセス

正解: A ([コメントを発表する](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 92

展示を参照してください。

```
snmp-server group SNMP v3 auth access 15
```

この構成では、15という数字は何を表していますか？

A. SNMPv3認証の試行間の秒単位の間隔

B. SNMPv3ユーザーがロックアウトされるまでに失敗した可能性のある試行の数

C. ルーターにアクセスできるSNMPデバイスを識別するアクセスリスト

D. このルーターに対する許可されたユーザーの特権レベル

正解: ([正解を表示します](#))

質問: 93

構成されたポスチャポリシー要件が満たされていない場合、どのコンプライアンスステータスが表示されますか？

A. 準拠

B. 不明

C. 承認済み

D. 非準拠

正解: ([正解を表示します](#))

ポスチャは、Cisco Identity Services Engine (Cisco ISE)のサービスであり、企業のセキュリティポリシーに準拠しているかどうか、ネットワークに接続しているすべてのエンドポイントの状態 (ポスチャとも呼ばれます)を確認できます。

ポスチャポリシーは、1つ以上のIDグループおよびオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。

ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。

+必須要件が満たされない場合、ユーザーは非準拠状態に移行します

+オプションの要件が失敗した場合、ユーザーは指定されたオプションの要件をスキップでき、ユーザーは準拠状態に移行します。このQdidは、姿勢ポリシー要件のタイプ（必須またはオプション）が満たされていないため、ユーザーは非準拠または準拠状態。ただし、ここでは「非準拠」が最善の答えです。

ポスチャは、Cisco Identity Services Engine (Cisco ISE)のサービスであり、企業のセキュリティポリシーに準拠しているかどうか、ネットワークに接続しているすべてのエンドポイントの状態（ポスチャとも呼ばれます）を確認できます。

ポスチャポリシーは、1つ以上のIDグループおよびオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。

ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。

+必須要件が満たされない場合、ユーザーは非準拠状態に移行します

+オプションの要件が失敗した場合、ユーザーは指定されたオプションの要件をスキップでき、ユーザーは準拠状態に移行します。このQdidは、姿勢ポリシー要件のタイプ（必須またはオプション）が満たされていないため、ユーザーは非準拠または準拠状態。ただし、ここでは「非準拠」が最善の答えです。

参照：

b_ise_admin_guide_sample_chapter_010111.html

ポスチャは、Cisco Identity Services Engine (Cisco ISE)のサービスであり、企業のセキュリティポリシーに準拠しているかどうか、ネットワークに接続しているすべてのエンドポイントの状態（ポスチャとも呼ばれます）を確認できます。

ポスチャポリシーは、1つ以上のIDグループおよびオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。

ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。

+必須要件が満たされない場合、ユーザーは非準拠状態に移行します

+オプションの要件が失敗した場合、ユーザーは指定されたオプションの要件をスキップでき、ユーザーは準拠状態に移行します。このQdidは、姿勢ポリシー要件のタイプ（必須またはオプション）が満たされていないため、ユーザーは非準拠または準拠状態。ただし、ここでは「非準拠」が最善の答えです。

b_ise_admin_guide_sample_chapter_010111.html

質問: 94

断片化されたパケットを使用してターゲットマシンをクラッシュさせる攻撃はどれですか？

A. 土地

B. ティアドロップ

C. MITM

D. スマーフ

正解: ([正解を表示します](#))

質問: 95

姿勢評価フローアクションを左から右のシーケンスにドラッグアンドドロップします。

Validate user credentials	step 1
Check device compliance with security policy	step 2
Grant appropriate access with compliant device	step 3
Apply updates or take other necessary action	step 4
Permit just enough for the posture assessment	step 5

正解:

Validate user credentials	Validate user credentials
Check device compliance with security policy	Permit just enough for the posture assessment
Grant appropriate access with compliant device	Check device compliance with security policy
Apply updates or take other necessary action	Apply updates or take other necessary action
Permit just enough for the posture assessment	Grant appropriate access with compliant device

質問: 96

ソリューションを左側から右側のソリューションのメリットにドラッグアンドドロップします。

Cisco Stealthwatch	obtains contextual identity and profiles for all the users and devices connected on a network.
Cisco ISE	software-defined segmentation that uses SGTs and allows administrators to quickly scale and enforce policies across the network
Cisco TrustSec	rapidly collects and analyzes NetFlow and telemetry data to deliver in-depth visibility and understanding of network traffic
Cisco Umbrella	secure Internet gateway in the cloud that provides a security solution that protects endpoints on and off the network against threats on the Internet by using DNS

正解:



質問: 97

Cisco AnyConnect VPNを使用するときに、最も強力なスループットパフォーマンスを提供するプロトコルはどれですか。

- A. TLSv1.2
- B. TLSv1.1
- C. BJTLSv1
- D. DTLSv1

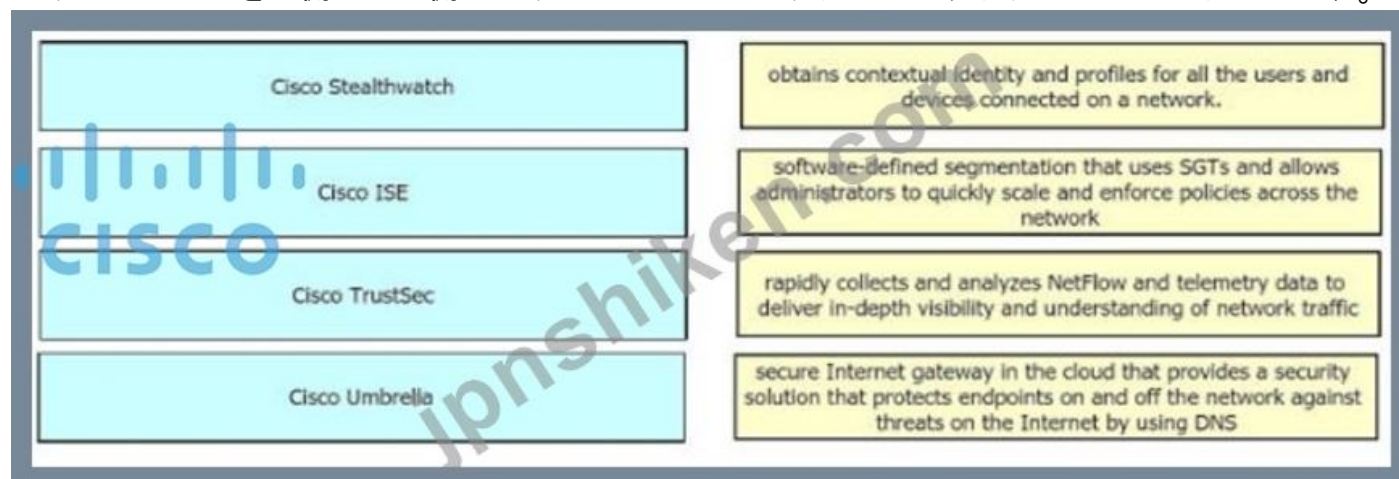
正解: [\(正解を表示します\)](#)

説明

DTLSはUDPベースであるため、遅延に敏感なアプリケーション（音声およびビデオ）に使用されますが、TLSはTCPベースです。したがって、DTLSは最強のスループットパフォーマンスを提供します。AnyConnect接続時のDTLSのスループットは、VPNスループットに近い処理パフォーマンスが期待できます。

質問: 98

ソリューションを左側から右側のソリューションのメリットにドラッグアンドドロップします。



正解:



Explanation:

Cisco Stealthwatch-ネットワークとテレメンティデータを迅速に収集および分析して、ネットワークトラフィックの詳細な可視性と理解を提供します
Cisco ISE-すべてのユーザーとデバイスのコンテキストIDとプロファイルを取得しますCisco TrustSec-SGTを使用するソフトウェア定義のセグメンテーション
Cisco Umbrella-安全なインターネットゲートウェイセキュリティソリューションを提供するクラウドをイオン化する

質問: 99

ネットワークエンジニアは、ネットワークに新しい医療機器を追加する任務を負っています。Cisco ISEはSheNACサーバとして使用されており、新しいデバイスには利用可能なサブリカントがありません。このデバイスをネットワークに安全に接続するには、何をする必要がありますか？

- A. プロファイリングでMABを使用する
- B. 姿勢評価でMABを使用します。
- C. 姿勢評価で802.1Xを使用します。
- D. プロファイリングで802.1Xを使用します。

正解: ([正解を表示します](#))

説明

新しいデバイスにはサブリカントがないため、802.1Xを使用できません。

MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。

Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意的識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。

分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づいて、ユーザーに差別化されたネットワークアクセスを提供することです。たとえば、従業員は会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。

質問: 100

組織には、Webアプリケーションをホストする2台のマシンがあります。マシン1はSQLインジェクションに対して脆弱ですが、マシン2はバッファオーバーフローに対して脆弱です。攻撃者がマシン1にアクセスできるが、マシン2にはアクセスできないようにするアクションは何ですか？

- A. 2つのホスト間のパケットをスニффイングする
- B. 継続的なpingの送信
- C. バッファのメモリがオーバーフローしました
- D. 悪意のあるコマンドをデータベースに挿入する

正解: [\(正解を表示します\)](#)

参照：

often used to dynamically build SQL statements that interact directly with a database. A SQL injection attack is an attack that is aimed at subverting the original intent of the application by submitting attacker-supplied SQL statements directly to the backend database. Depending on the web application, and how it

質問: 101

NetFlowエクスポートフォーマットを左から右の説明にドラッグアンドドロップします。

Version 1	appropriate only for the main cache
Version 5	introduced support for aggregation caches
Version 8	appropriate only for legacy systems
Version 9	introduced extensibility

正解:

Version 1	Version 5	
Version 5	Version 8	hes
Version 8	Version 1	
Version 9	Version 9	

質問: 102

ソフトウェア定義のネットワークアーキテクチャ内のコントローラーがネットワーク内のスイッチの構成を動的に変更する場合、どのタイプのAPIが使用されますか？

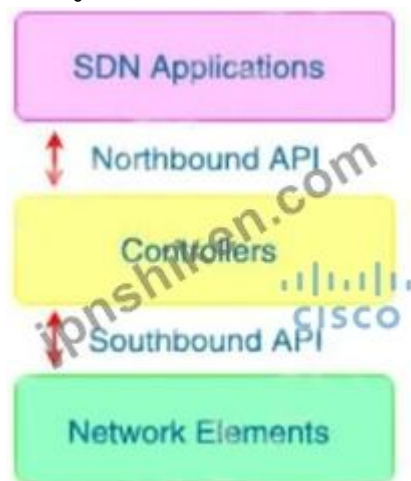
- A. 西行きAP
- B. サウスバウンドAPI
- C. ノースバウンドAPI
- D. イーストバウンドAPI

正解: ([正解を表示します](#))

説明

説明

サウスバウンドAPIを使用すると、SDNコントローラーはリアルタイムの要求とスケーラビリティのニーズに基づいて動的に変更を加えることができます。



質問: 103

可能な限り強力なセキュリティをサポートするには、どのSNMPv3構成を使用する必要がありますか？

A. asa-host (config) #snmp-server group myv3 v3 priv

asa-host (config) #snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host (config) #snmp-server host inside 10.255.254.1 version 3 andy

B. asa-host (config) #snmp-server group myv3 v3 noauth

asa-host (config) #snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host (config) #snmp-server host inside 10.255.254.1 version 3 andy

C. asa-host (config) #snmp-server group myv3 v3 priv

asa-host (config) #snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXXX asa-host (config) #snmp-server host inside 10.255.254.1 version 3 andy

D. asa-host (config) #snmp-server group myv3 v3 noauth

asa-host (config) #snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXXX asa-host (config) #snmp-server host inside 10.255.254.1 version 3 andy

正解: ([正解を表示します](#))

質問: 104

クラウドベースのソリューションよりもオンプレミスのソリューションを選択する場合、どの要素を考慮する必要がありますか？

A. オンプレミスソリューションでは、プロバイダーが製品のインストールとメンテナンスを担当しますが、クラウドベースのソリューションでは、顧客が責任を負います。

B. クラウドベースのソリューションでは、プロバイダーがインストールの責任を負いますが、顧客は製品のメンテナンスの責任を負います。

C. オンプレミスソリューションでは、プロバイダーがインストールの責任を負いますが、顧客は製品のメンテナンスの責任を負います。

D. オンプレミスソリューションでは、お客様がインストールとメンテナンスの責任を負います

正解: ([正解を表示します](#))

製品ですが、クラウドベースのソリューションでは、プロバイダーが責任を負います。

質問: 105

説明を左側から右側の暗号化アルゴリズムにドラッグアンドドロップします。

requires secret keys

requires more time

Diffie-Hellman exchange

3DES

Asymmetric

Symmetric

正解:

requires secret keys

requires more time

Diffie-Hellman exchange

3DES

Asymmetric

requires secret keys

Diffie-Hellman exchange

Symmetric

requires more time

3DES

質問: 106

CiscoFirepowerのセキュリティインテリジェンスポリシーを使用します。Firepowerブロックベースの2つの基準はどれですか。2つ選択してください。)

- A. プロトコルID
- B. URL
- C. IPアドレス
- D. ポート番号
- E. MACアドレス

正解: (正解を表示します)

参照 :

Security Intelligence Sources

- System-provided feeds
- Cisco provides access to regularly updated intelligence feeds for domains, URLs and IP addresses.

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **107**

組織にポリシーが設定されたCiscoESAがあり、違反に割り当てられたアクションをカスタマイズしたいと考えています。組織は、DLP違反としてフラグを立てるためにメッセージを追加して、メッセージのコピーを配信することを望んでいます。この機能を提供するには、どのアクションを実行する必要がありますか？

- A. 免責事項のテキストを配信して追加する
- B. DLP違反通知を隔離して送信します
- C. 他の受信者にコピーを配信して送信する
- D. DLP違反でサブジェクトヘッダーを隔離および変更します

正解: ([正解を表示します](#))

質問: **108**

NetFlowフローモニタリングの2つの機能は何ですか？ 2つ選択してください

- A. 入力および出力情報を追跡できます
- B. フローレコードとフローインポーターを含める
- C. すべての入力フロー情報をインターフェースにコピーします
- D. インターフェイスでのパケットサンプリングは必要ありません
- E. マルチキャスト、MPLS、またはブリッジトラフィックの追跡に使用できます

正解: ([正解を表示します](#))

以下は、Flexible NetFlowの制限事項です。+従来のNetFlow (NF) アカウンティングはサポートされていません。+フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。+入力と出力の両方のNetFlowアカウンティングがサポートされています。+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。+インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。参照：

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/solidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html

NetFlowを設定するときは、次のガイドラインと制限に従ってください。+PFC3Aモードを除く、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。+NetFlowはマルチキャストIPトラフィックをサポートします。参照：https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.htmlフレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルーターに到着するパケットのIPフロー情報をマルチプロトコルラベルスイッチング (MPLS) パケットとしてキャプチャできます。IPパケットとして送信されます。この機能を使用すると、サービスプロバイダバックボーンを介してVPNのあるサイトから同じVPNの別のサイトに移動するMPLS VPN IPフローをキャプチャできます。<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html>

+従来のNetFlow (NF) アカウンティングはサポートされていません。

+フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。

+入力と出力の両方のNetFlowアカウンティングがサポートされています。

+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。

+インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。

参照：

[Consolidated_guide / b_consolidated_3850_3se_cg_chapter_011010.html](#)

NetFlowを設定するときは、次のガイドラインと制限に従ってください。

+ PFC3Aモードを除いて、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。

+NetFlowはマルチキャストIPトラフィックをサポートします。

フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、VPNのあるサイトから同じVPNの別のサイトにサービスプロバイダーバックボーンを通過するMPLS VPNIPフローをキャプチャできます。FlexibleNetFlowの制限は次のとおりです。+従来のNetFlow (TNF) アカウンティングはサポートされていません。。+フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。+入力と出力の両方のNetFlowアカウンティングがサポートされています。+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。+インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。参照：

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/Consolidated_guide/

[b_consolidated_3850_3se_cg_chapter_011010.html](#) NetFlowを設定するときは、次のガイドラインと制限に従ってください。+ PFC3Aモードを除

き、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。+NetFlowはマルチキャストIPトラフィックをサポートします。参照 https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、マルチプロトコルラベルスイッチング (MPLS) パケットとしてルーターを使用し、IPパケットとして送信されます。この機能を使用すると、VPNのあるサイトから同じVPNリファレンスの別のサイト (<https://www.cisco.com>) にサービスプロバイダーバックボーンを通過するMPLSVPNIPフローをキャプチャできます。

質問: 109

エンドポイント向けの十分に確立されたパッチソリューションがない場合、企業が脆弱になる2つのリスクはどれですか。2つ選択してください。

A. ARPスプーフィング

B. 盗聴

C. サービス拒否攻撃

D. エクスプロイト

E. マルウェア

正解: ([正解を表示します](#))

質問: 110

攻撃者は、相互に通信している2つのホストの間に、どのタイプの攻撃でマシンを挿入しますか？

A. LDAPインジェクション

B. クロスサイトスクリプティング

C. 中間者

D. 安全でないAPI

正解: ([正解を表示します](#))

参照：

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

質問: 111

管理者は、ネットワークで使用されているアプリケーションを特定しようとしていますが、ネットワークデバイスがCiscoFirepowerにメタデータを送信することを望んでいません。これを実現するには、どの機能を使用する必要がありますか？

- A. NetFlow
- B. パケットトレーサー
- C. ネットワークディスクバリー
- D. アクセス制御

正解: ([正解を表示します](#))

NetFlowは、NetFlow対応のルーターおよびスイッチによって生成されたネットワークトラフィックフローデータを収集および監視するためにシスコが開発したネットワークプロトコルです。フローには実際のパケットデータは含まれていませんが、通信用のメタデータが含まれています。これは、ネットワークトラフィックの誰が、何を、いつ、どこで行うかを詳細に示すセッションデータの標準形式です-回答Aは正しくありません。参照 :NetFlow対応ルーターおよびスイッチによって生成された<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html>。フローには実際のパケットデータは含まれていませんが、通信用のメタデータが含まれています。これは、ネットワークトラフィックの誰が、何を、いつ、どこで行うかを詳細に示すセッションデータの標準形式です-回答Aは正しくありません。

参照 :

NetFlowは、NetFlow対応のルーターおよびスイッチによって生成されたネットワークトラフィックフローデータを収集および監視するためにシスコが開発したネットワークプロトコルです。フローには実際のパケットデータは含まれていませんが、通信用のメタデータが含まれています。これは、ネットワークトラフィックの誰が、何を、いつ、どこで行うかを詳細に示すセッションデータの標準形式です-回答Aは正しくありません。参照 :
<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html>

質問: 112

どのIPSエンジンがARPスプーフィングを検出しますか？

- A. ARP検査エンジン
- B. サービスジェネリックエンジン
- C. アトミックARPエンジン
- D. AICエンジン

正解: ([正解を表示します](#))

質問: 113

Cisco ESA管理者は、隔離された電子メールが配信される前にウイルスがないことを確認するようにCiscoESAを設定する必要があります。さらに、既知の不良メールサーバーからのメールの配信を防止する必要があります。これらの要件を満たすために実行する必要がある2つのアクションはどれですか？ 2つ選択してください)

- A. SenderBaseのアウトブレイクフィルターを使用する
- B. メッセージ追跡サービスを有効にする
- C. 受信者アクセステーブルを設定します
- D. CiscoESAをDMZに導入します
- E. アンチウイルス署名を使用して隔離された電子メールをスキャンする

正解: **A,E** ([コメントを发表する](#))

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。参照 https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html->

したがって、アウトブレイクフィルターを使用して、不良メールサーバーからの電子メールをブロックできます。Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、注 :リモートアクセストロイの木馬 (RAT)と混同しないように、受信者アクセステーブル (RAT)は、どの受信者が一般に受け入れられるかを定義するCiscoESA用語です。リスナー。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

参照 :

[b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html](https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html)

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。参照 https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html->

したがって、アウトブレイクフィルターを使用して、不良メールサーバーからの電子メールをブロックできます。Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、注 :リモートアクセストロイの木馬 (RAT)と混同しないように、受信者アクセステーブル (RAT)は、どの受信者が一般に受け入れられるかを定義するCiscoESA用語です。リスナー。

質問: **114**

組織のDMZには2つのシステムがあり、通信のためにそれらの間に暗号化されていないリンクがあります。

組織には定義済みのパスワードポリシーがなく、システムでいくつかのデフォルトアカウントを使用しています。

これらのシステムで使用されているアプリケーションも、厳格なコードレビューを受けていません。攻撃者がブルートフォースでシステムに侵入するのに役立つ脆弱性はどれですか？

- A. 弱いパスワード
- B. 入力検証の欠如
- C. 暗号化がありません
- D. ファイル権限の欠如

正解: [\(正解を表示します\)](#)

説明バージョン9のエクスポート形式では、テンプレートを使用して、柔軟かつ拡張可能な方法でIPパケットフローの監視へのアクセスを提供します。テンプレートは、構造とセマンティクスの対応する説明とともに、フィールドのコレクションを定義します。参照 <https://tools.ietf.org/html/rfc3954>バージョン9のエクスポート形式では、テンプレートを使用して、柔軟かつ拡張可能な方法でIPパケットフローの監視にアクセスできます。テンプレートは、構造とセマンティクスの対応する説明とともに、フィールドのコレクションを定義します。説明バージョン9のエクスポート形式では、テンプレートを使用して、柔軟かつ拡張可能な方法でIPパケットフローの監視へのアクセスを提供します。テンプレートは、構造とセマンティクスの対応する説明とともに、フィールドのコレクションを定義します。参照 <https://tools.ietf.org/html/rfc3954>

質問: 115

クロスサイトスクリプティングを制御するために使用される2つの予防策はどれですか？ 2つ選択してください。)

- A. 信頼できないHTML入力をHTMLサニタイズエンジンを介して実行します。
- B. ドメインごとにクライアント側のスクリプトを有効にします。
- C. SameSitecookie属性は使用しないでください。
- D. HTMLインスペクションエンジンでCookieインスペクションを無効にします。
- E. コンテキスト出力のエンコーディング/エスケープを組み込みます。

正解: [\(正解を表示します\)](#)

質問: 116

一般的なセキュリティの脅威を左側から右側の定義にドラッグアンドドロップします。

phishing	a software program that copies itself from one computer to another, without human interaction
botnet	unwanted messages in an email inbox
spam	group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse
worm	fraudulent attempts by cyber criminals to obtain private information

正解:



質問: 117

展示を参照してください。

この出力を生成し、どのポートがdot1xまたはmabで認証されているかを示すために使用されたコマンドはどれですか。

- A. 認証方法を表示
- B. dot1xallを表示
- C. 認証セッションを表示
- D. 認証登録を表示する

正解: B ([コメントを發表する](#))

質問: 118

エンジニアがカスタム検出ポリシーをCiscoAMP展開に追加し、設定で問題が発生した単純な検出メカニズムが設定されていますが、ダッシュボードにハッシュが64文字ではなく、ゼロ以外であることが示されています。問題は何ですか。

- A. エンジニアがハッシュではなくファイルをアップロードしようとしています
- B. エンジニアがSHA-256の代わりにMD5を使用して作成されたハッシュをアップロードしようとしています
- C. アップロードされているハッシュが誤った形式のセットの一部です
- D. アップロードされるファイルは単純な検出と互換性がなく、高度な検出を使用する必要があります

正解: ([正解を表示します](#))

質問: 119

AdvancedThreatStatistics以外の脅威検出機能を無効にするCiscoASAプラットフォームモードはどれですか。

- A. クラスタ
- B. 複数のコンテキスト
- C. ルーティング
- D. 透明

正解: ([正解を表示します](#))

質問: 120

SDNサウスバウンドAPIプロトコルの機能は何ですか？

- A. コントロールプレーンアプリケーションの動的構成を可能にするため
- B. コントローラーが変更を行えるようにする

C. コントローラーがRESTを使用できるようにします

D. コントロールプレーンアプリケーションの静的構成を可能にするため

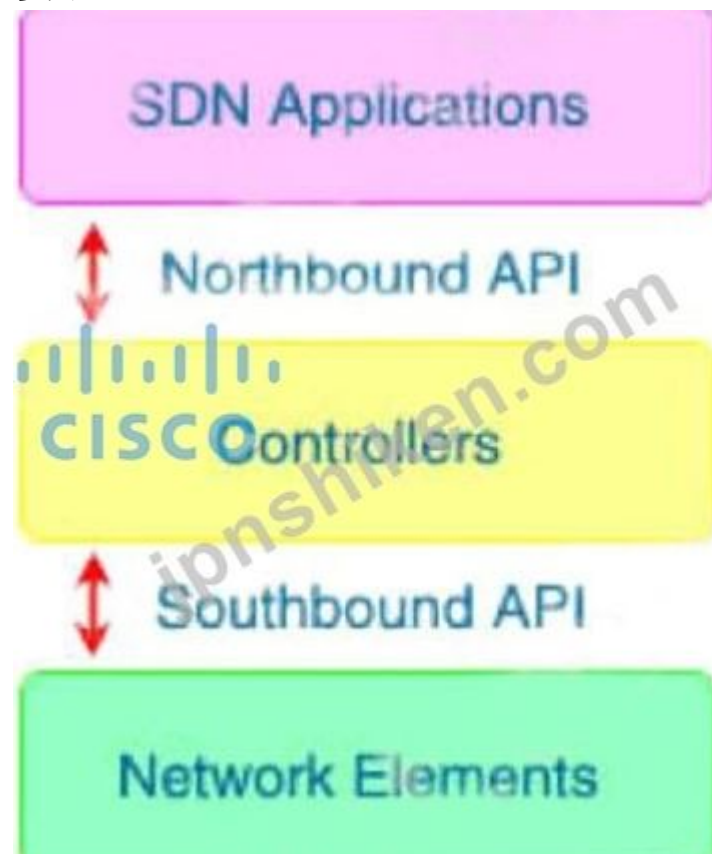
正解: (正解を表示します)

サウスバウンドAPIを使用すると、SDNコントローラーはリアルタイムの要求とスケーラビリティのニーズに基づいて動的に変更を加えることができます。

サウスバウンドAPIを使用すると、SDNコントローラーはリアルタイムの要求とスケーラビリティのニーズに基づいて動的に変更を加えることができます。

サウスバウンドAPIを使用すると、SDNコントローラーはリアルタイムの要求とスケーラビリティのニーズに基づいて動的に変更を加えることができます。

参照：



注 :サウスバウンドAPIは、データプレーン (コントロールプレーンではない)アプリケーションとの通信に役立ちます

質問: 121

RADIUS CoA中に変更できる属性はどれですか？

A. NTP

B. 承認

C. アクセシビリティ

D. メンバーシップ

正解: (正解を表示します)

RADIUSの許可変更 (CoA) 機能は、認証後に認証、許可、およびアカウントिंग (AAA) セッションの属性を変更するメカニズムを提供します。参照：

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-認証後のrad-coa.html 認証、許可、およびアカウントिंग (AAA) セッション。

参照：

RADIUSの許可変更 (CoA) 機能は、認証後に認証、許可、およびアカウントिंग (AAA) セッションの属性を変更するメカニズムを提供します。参照：
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **122**

展示を参照してください。

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
description Uplink_To_Distro_Switch_g1/0/11
switchport trunk native vlan 999
switchport trunk allowed vlan 40,41,44
switchport mode trunk
```

組織は、ネットワーク内でDHCPスヌーピングを使用しています。新しいスイッチのVLAN41のユーザーが、IPアドレスが取得されていないと不満を言っています。ユーザーにネットワーク接続を提供するために、スイッチインターフェイスでどのコマンドを設定する必要がありますか？

- A. ip dhcp snooping verify mac-address
- B. ip dhcp snooping limit 41
- C. ip dhcp snooping vlan 41
- D. ip dhcp snooping trust

正解: ([正解を表示します](#))

説明

説明

DHCPスヌーピングを理解するには、最初にDHCPスプーフィング攻撃について学ぶ必要があります。

DHCPスプーフィングは、攻撃者がクライアントからのDHCP要求をリッスンし、許可されたDHCP応答がクライアントに到達する前に、偽のDHCP応答で応答するという攻撃の一種です。偽のDHCP応答は、多くの場合、クライアントのデフォルトゲートウェイとしてIPアドレスを提供します-クライアントから送信されるすべてのトラフィックは攻撃者のコンピュータを通過し、攻撃者は「中間者」になります。

攻撃者は、偽のDHCP応答が最初に到着することを確認するいくつかの方法があります。実際、攻撃者がDHCPサーバーよりも「近い」場合、攻撃者は何もする必要はありません。または、DHCPサーバーをDoSして、DHCP応答を送信できないようにすることもできます。

DHCPスヌーピングは、DHCPスプーフィング攻撃を防ぐことができます。DHCPスヌーピングは、DHCP要求に応答できるスイッチポートを決定するCiscoCatalystの機能です。ポートは、信頼できるものと信頼できないものとして識別されます。

許可されたDHCPサーバーに接続するポートのみが信頼され、すべての種類のDHCPメッセージの送信が許可されます。スイッチ上の他のすべてのポートは信頼されておらず、DHCP要求のみを送信できます。信頼できないポートでDHCP応答が見られる場合、ポートはシャットダウンされます。

DHCPサーバーに接続されているポートは、`ipdhcpsnoopingtrust` コマンドを使用して信頼できるポートとして構成する必要があります。ホストに接続している他のポートは、デフォルトでは信頼できないポートです。
この質問では、以下に示すように、アップリンクを「信頼」(インターフェイスGi1 / 0/1の下)に構成する必要があります。

質問: 123

組織は、短期間に大量のスパムメッセージを受信しました。メッセージに対してアクションを実行するには、メッセージがどれほど有害であるかを判断する必要があります、これは動的に発生する必要があります。
これを実現するには何を構成する必要がありますか？

- A. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoWSAを設定します。
- B. Talosからリアルタイムアップデートを受信するようにCiscoESAを設定します
- C. Talosからリアルタイムアップデートを受信するようにCiscoWSAを設定します。
- D. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoESAを設定します。

正解: ([正解を表示します](#))

説明

https://www.cisco.com/c/en/us/td/docs/security/esa/esa120/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Adm

質問: 124

Cisco Email Securityの2つの機能のうち、電子メールの脅威から組織を保護できるのはどれですか。2つ選択してください)

- A. 時間ベースのワнтаムパスワード
- B. データ損失防止
- C. ヒューリスティックベースのフィルタリング
- D. ジオロケーションベースのフィルタリング
- E. NetFlow

正解: ([正解を表示します](#))

データ損失防止 (DLP) と使いやすい電子メール暗号化をすべて1つのソリューションで使用して、送信電子メールの機密コンテンツを保護します。
Cisco Email Securityアプライアンスは、特定の地理的位置からの着信メール接続と着信メッセージを処理し、それらに対して適切なアクションを実行できるようになりました。たとえば、次のようになります。

-特定の地理的地域からの電子メールの脅威を防ぎます。

-特定の地域からのメールを許可または禁止します。

データ損失防止 (DLP) と使いやすい電子メール暗号化をすべて1つのソリューションで使用して、送信電子メールの機密コンテンツを保護します。
Cisco Email Securityアプライアンスは、特定の地理的位置からの着信メール接続と着信メッセージを処理し、それらに対して適切なアクションを実行できるようになりました。たとえば、次のようになります。

-特定の地理的地域からの電子メールの脅威を防ぎます。

-特定の地域からのメールを許可または禁止します。

参照 :

[b_ESA_Admin_Guide_11_0 / b_ESA_Admin_Guide_chapter_00.html](#)

データ損失防止 (DLP) と使いやすい電子メール暗号化をすべて1つのソリューションで使用して、送信電子メールの機密コンテンツを保護します。
Cisco Email Securityアプライアンスは、特定の地理的位置からの着信メール接続と着信メッセージを処理し、それらに対して適切なアクションを実行できるようになりました。たとえば、次のようになります。

-特定の地理的地域からの電子メールの脅威を防ぎます。

-特定の地域からのメールを許可または禁止します。

b_ESA_Admin_Guide_11_0 / b_ESA_Admin_Guide_chapter_00.html

質問: 125

ステップを左から右の正しい順序にドラッグアンドドロップして、AppDynamicsがアマゾンウェブサービスのEC2インスタンスを監視できるようにします。

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

正解:

Install monitoring extension for AWS EC2.	Configure a Machine Agent or SIM Agent.
Restart the Machine Agent.	Install monitoring extension for AWS EC2.
Update config.yaml.	Update config.yaml.
Configure a Machine Agent or SIM Agent.	Restart the Machine Agent.

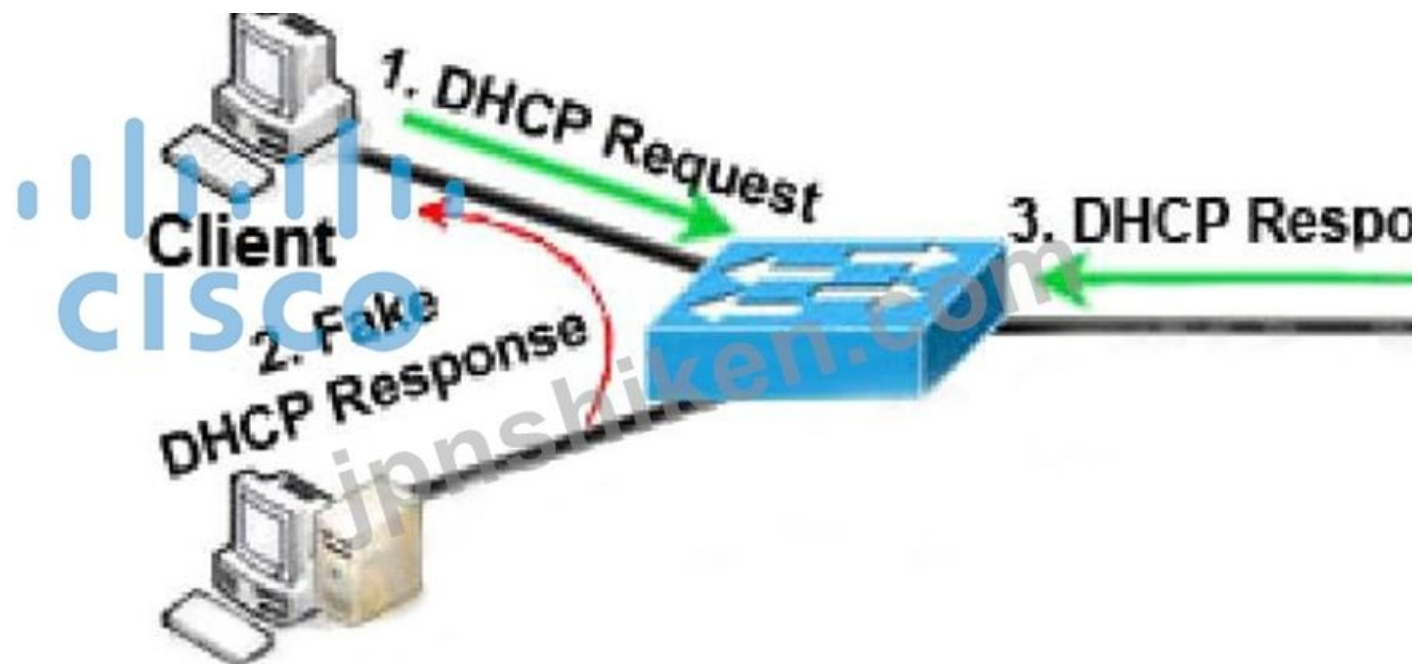
質問: 126

管理者は、環境をより安全にするためにDHCPサーバーを構成しています。トラフィックをレート制限し、正当な要求がドロップされないようにする必要があります。これはどのように達成されますか？

- A. DHCPサーバーの信頼できるインターフェースを設定します
- B. DHCPスヌーピングビットを1に設定します
- C. DHCPスヌーピングデータベースにエントリを追加します
- D. 必要なVLANのARP検査を有効にします

正解: ([正解を表示します](#))

DHCPスヌーピングを理解するには、最初にDHCPスプーフィング攻撃について学ぶ必要があります。

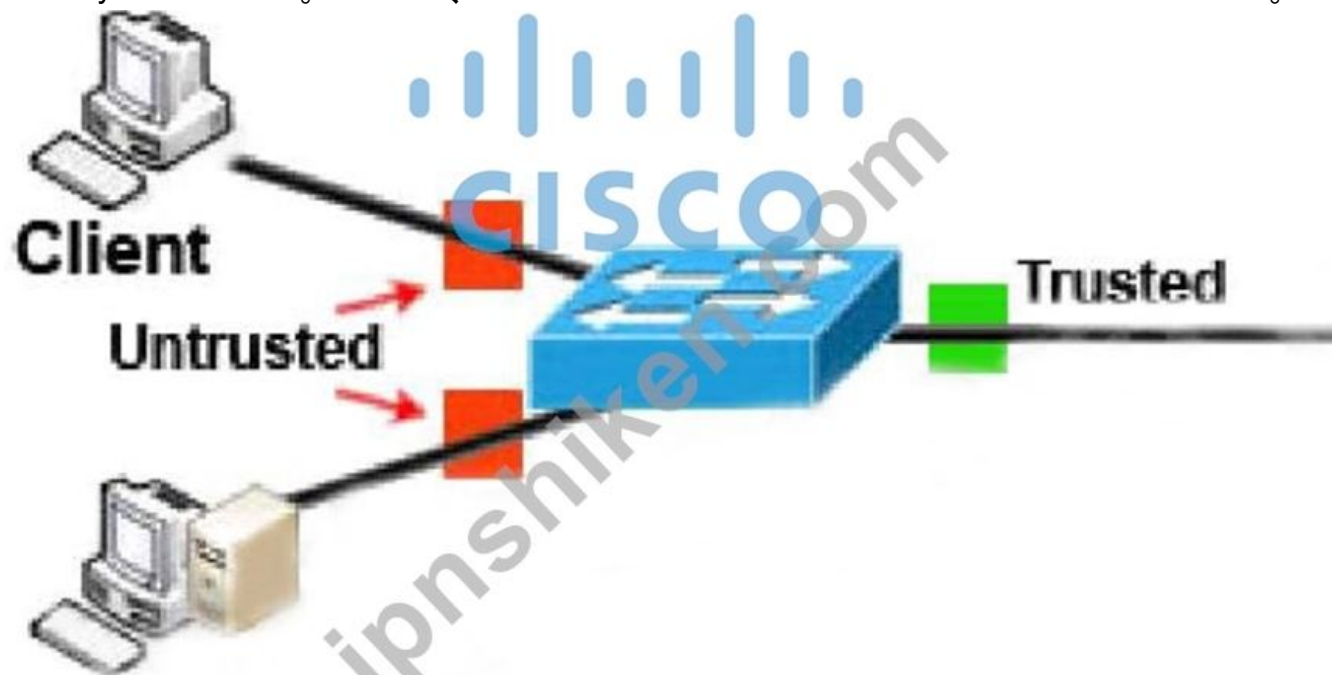


DHCP Attacker

DHCPスプーフィングは、攻撃者がクライアントからのDHCP要求をリッスンし、許可されたDHCP応答がクライアントに到達する前に、偽のDHCP応答で応答するという攻撃の一種です。偽のDHCP応答は、多くの場合、クライアントのデフォルトゲートウェイとしてIPアドレスを提供します。クライアントから送信されるすべてのトラフィックは攻撃者のコンピュータを通過し、攻撃者は「中間者」になります。

攻撃者は、偽のDHCP応答が最初に到着することを確認するいくつかの方法があります。実際、攻撃者がDHCPサーバーよりも「近い」場合、攻撃者は何もする必要はありません。または、DHCPサーバーをDoSして、DHCP応答を送信できないようにすることもできます。

DHCPスヌーピングは、DHCPスプーフィング攻撃を防ぐことができます。DHCPスヌーピングは、DHCP要求に応答できるスイッチポートを決定するCiscoCatalystの機能です。ポートは、信頼できるものと信頼できないものとして識別されます。

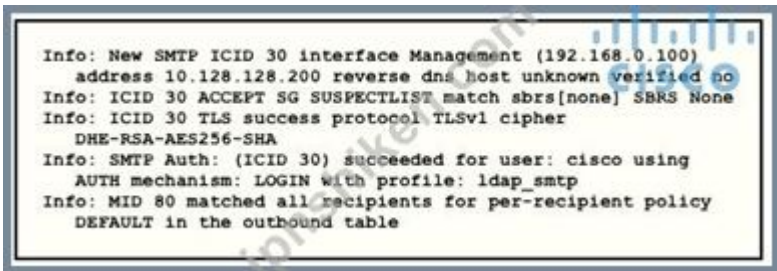


DHCP Attacker

許可されたDHCPサーバーに接続するポートのみが信頼され、すべての種類のDHCPメッセージの送信が許可されます。スイッチ上の他のすべてのポートは信頼されておらず、DHCP要求のみを送信できます。信頼できないポートでDHCP応答が見られる場合、ポートはシャットダウンされます。

質問: 127

R157



どのタイプの認証が使用されていますか？

- A. SMTPリレーサーバー認証
- B. POP3認証
- C. 外部ユーザーとリレーメール認証
- D. MicrosoftOutlookのLDAP認証

正解: D (コメントを发表する)

質問: 128

攻撃者は、DNSトンネリングを使用した抽出中に、DNS要求のデータをどの方向にエンコードしますか？

- A. 東西
- B. アウトバウンド
- C. 南北
- D. インバウンド

正解: B (コメントを发表する)

質問: 129

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

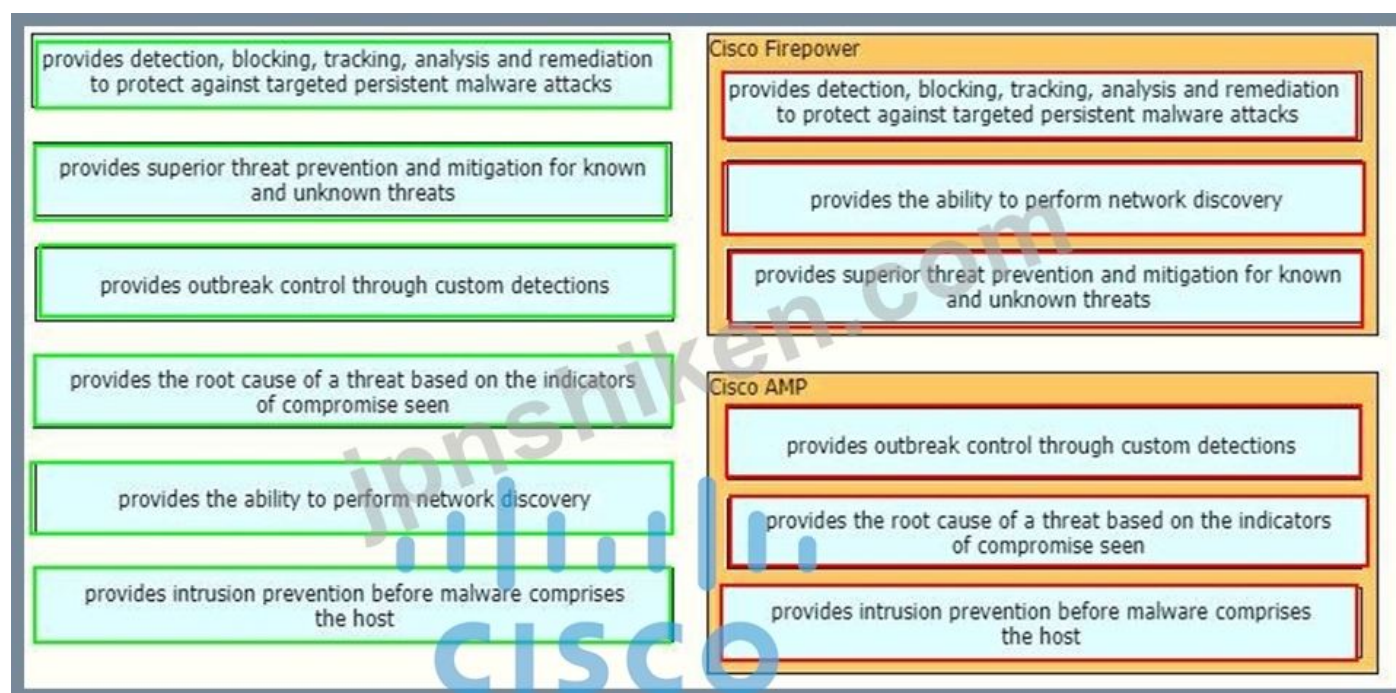
provides the ability to perform network discovery

provides intrusion prevention before malware compromises the host

Cisco Firepower

Cisco AMP

正解:



<https://www.cisco.com/c/en/us/products/collateral/security/ngips/datasheet-c78-742472.html>

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

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html>

質問: 130

CiscoFirepowerのセキュリティインテリジェンスポリシーを使用します。Firepowerブロックベースの2つの基準はどれですか。
(2つ選択してください)

- A. URL
- B. プロトコルID
- C. IPアドレス
- D. MACアドレス
- E. ポート番号

正解: (正解を表示します)

セキュリティインテリジェンスソース...カスタムブロックリストまたはフィード (またはオブジェクトまたはグループ) 手動で作成されたリストまたはフィードを使用して、特定のIPアドレス、URL、またはドメイン名をブロックします (IPアドレスの場合、ネットワークオブジェクトまたはグループを使用することもできます)。たとえば、フィードによってまだブロックされていない悪意のあるサイトまたはアドレスに気付いた場合は、これらのサイトをカスタムセキュリティインテリジェンスリストに追加し、このカスタムリストをアクセス制御ポリシーの[セキュリティインテリジェンス]タブのブロックリストに追加します。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/security_intelligence_blacklisting.html

..。

カスタムブロックリストまたはフィード (またはオブジェクトまたはグループ)

手動で作成したリストまたはフィードを使用して、特定のIPアドレス、URL、またはドメイン名をブロックします (IPアドレスの場合、ネットワークオブジェクトまたはグループを使用することもできます)。たとえば、悪意のあるサイトまたはまだブロックされていないアドレスに気付いた場合フィードを使用して、これらのサイトをカスタムセキュリティインテリジェンスリストに追加し、このカスタムリストをアクセス制御ポリシーの[セキュリティインテリジェンス]タブの[ブロック]リストに追加します。

セキュリティインテリジェンスソース...カスタムブロックリストまたはフィード またはオブジェクトまたはグループ) 手動で作成されたリストまたはフィードを使用して、特定のIPアドレス、URL、またはドメイン名をブロックします IPアドレスの場合、ネットワークオブジェクトまたはグループを使用することもできます)。たとえば、フィードによってまだブロックされていない悪意のあるサイトまたはアドレスに気付いた場合は、これらのサイトをカスタムセキュリティインテリジェンスリストに追加し、このカスタムリストをアクセス制御ポリシーの[セキュリティインテリジェンス]タブのブロックリストに追加します。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/security_intelligence_blacklisting.html

質問: 131

Cloudlock Apps Firewallは、アプリケーションの観点からセキュリティ上の懸念を軽減するために何をしますか？

- A. 企業の企業環境に接続されているクラウドアプリを検出して制御します。
- B. アプリケーション情報を管理者に送信して対処します。
- C. ネットワークに属していないアプリケーションを削除します。
- D. 管理者が悪意のあるファイルを隔離して、アプリケーションが悪意を持ってではなく機能できるようにします。

正解: ([正解を表示します](#))

質問: 132

Cisco FTDvはASA vに対してどのような機能を提供しますか？

- A. Cisco FTDvはURLフィルタリングをサポートしていますが、ASA vはサポートしていません。
- B. Cisco FTDvはAWSで実行されますが、Cisco ASA vは実行されません。
- C. Cisco FTDvはIGBのファイアウォールスルーputを提供しますが、Cisco ASA vは提供しません。
- D. Cisco FTDvはVMWareで実行されますが、Cisco ASA vは実行されません。

正解: ([正解を表示します](#))

質問: 133

ハイブリッド電子メールソリューションを導入する場合、オンプレミス機器として残しておく必要がある2つのサービスはどれですか。(2つ選択してください。)

- A. ウイルス対策
- B. DDoS
- C. 暗号化
- D. DLP
- E. スпам対策

正解: ([正解を表示します](#))

質問: 134

インラインポスチャノードを必要とせずに、VPNユーザーがCisco ISEに対してポスチャできるCisco ASAの機能はどれですか。

- A. RADIUSの承認変更
- B. DHCPスヌーピング
- C. デバイス追跡
- D. VLANホッピング

正解: A ([コメントを发表する](#))

質問: 135

ボットネットを使用して開始される攻撃の形式はどれですか？

- A. TCPフラッド
- B. ODOS
- C. EIDDOS
- D. ウイルス

正解: ([正解を表示します](#))

質問: 136

エンジニアがMicrosoftWindowsエンドポイントでポスチャチェックを使用し、MS17-010パッチがインストールされていないことを発見しました。これにより、エンドポイントがWannaCryランサムウェアに対して脆弱なままになりました。

このランサムウェア感染のリスクを軽減する2つのソリューションはどれですか？ 2つ選択してください。)

- A. ネットワークへのアクセスを許可する前にエンドポイントパッチレベルが満たされていることを確認するために、Cisco IdentityServicesEngineでポスチャポリシーを設定します。
- B. 明確に定義されたエンドポイントのパッチ適用戦略を設定して、エンドポイントに重大な脆弱性にタイムリーにパッチが適用されるようにします。
- C. ネットワークへのアクセスを許可する前にMS17-010パッチをインストールするようにCisco IdentityServicesEngineでポスチャポリシーを設定します。
- D. ネットワークへのアクセスを許可する前にエンドポイントパッチレベルをチェックするように、Cisco IdentityServicesEngineでプロファイリングポリシーを設定します。
- E. エンドポイントファイアウォールポリシーを構成して、エクスプロイトトラフィックの実行とネットワーク全体での複製が許可されないようにします。

正解: ([正解を表示します](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 137

どのMDM構成がスケーラビリティを提供しますか？

- A. カメラの使用などのデバイス機能の使用を有効にする
- B. レベル7のフィンガープリントによる自動デバイス分類
- C. 追加のアプライアンスまたはライセンスなしのBYODサポート
- D. WPA2-Enterprise設定をデバイスに自動的にプッシュする

正解: C ([コメントを发表する](#))

質問: 138

CiscoFirepowerとCiscoASAの主な違いは何ですか。

- A. Cisco ASAはSSL検査を提供しますが、CiscoFirepowerは提供しません。
- B. Cisco Firepowerはネイティブに侵入防止機能を提供しますが、CiscoASAは提供しません。
- C. Cisco ASAはアクセス制御を提供しますが、CiscoFirepowerは提供しません。
- D. Cisco FirepowerはIDベースのアクセス制御を提供しますが、CiscoASAは提供しません。

正解: B ([コメントを发表する](#))

質問: 139

展示を参照してください。

```
HQ_Router(config)# username admin5 privilege 5
HQ_Router(config)#privilege interface level 5 shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5 description
```

ネットワーク管理者は、admm5ユーザーのコマンド認証を構成します。この設定後、admin5ユーザーはHQ_Routerで何ができますか？

- A. サブインターフェースを追加
- B. インターフェースのIPアドレスを設定します
- C. すべての構成を完了する
- D. 構成を完了しない

正解: ([正解を表示します](#))

質問: 140

ソリューションを左側から右側のソリューションのメリットにドラッグアンドドロップします。

Cisco Stealthwatch	obtains contextual identity and profiles for all the users and devices connected on a network.
Cisco ISE	software-defined segmentation that uses SGTs and allows administrators to quickly scale and enforce policies across the network
Cisco TrustSec	rapidly collects and analyzes NetFlow and telemetry data to deliver in-depth visibility and understanding of network traffic
Cisco Umbrella	secure Internet gateway in the cloud that provides a security solution that protects endpoints on and off the network against threats on the Internet by using DNS

正解:



質問: 141

エンジニアがエンドポイントでのファイルやプロセスのアクティビティなど、過去のアクティビティを追跡できるCiscoAMP機能はどれですか。

- A. 高度な調査
- B. 遡及的セキュリティ
- C. エンドポイントの分離
- D. 高度な検索

正解: ([正解を表示します](#))

質問: 142

Cisco IOSルータでIKEv1Phase1のISAKMPを設定する場合、管理者はコマンドcrypto isakmp key ciscoaddress0.0.0.0を入力する必要があります。管理者は、このコマンドのIPアドレスが何のために発行されたのかわかりません。IPアドレスを0.0.0.0から1.2.3.4に変更するとどのような影響がありますか？

- A. 接続用のキーを管理しているキーサーバーは1.2.3.4になります
- B. リモート接続は1.2.3.4からのみ許可されます
- C. 暗号検証機関として使用されるアドレス
- D. 1.2.3.4以外のすべてのIPアドレスが許可されます

正解: ([正解を表示します](#))

説明コマンドcryptoisakmpkey cisco address 1.2.3.4は、キーciscoを使用して1.2.3.4ピアのIPアドレスを認証します。0.0.0.0のアドレスは、このキーですべてのアドレスを認証します

質問: 143

Cisco WSAでPACファイルを使用する際に考慮すべき2つのことは何ですか？ (2つ選択してください。)

- A. WSAは、デフォルトでポート6001でPACファイルをホストします。
- B. WSAは、デフォルトでポート9001でPACファイルをホストします。
- C. デフォルトでは、PCとホストが同じサブネット上にある場合、トラフィックはプロキシ経由で転送されます。
- D. WSAホストポートが変更された場合、デフォルトのポートはWebトラフィックを正しいポートに自動的にリダイレクトします。
- E. PACファイルはif-elseステートメントを使用して、PCとホスト間のトラフィックにプロキシを使用するか直接接続を使用するかを決定します。

正解: ([正解を表示します](#))

質問: 144

公開鍵と秘密鍵を使用する暗号化のタイプはどれですか？

- A. 対称
- B. 線形
- C. 非線形
- D. 非対称

正解: D ([コメントを发表する](#))

質問: 145

組織内にMFAを実装することが重要なのはなぜですか？

- A. フィッシング攻撃の成功を防ぐため。
- B. DoS攻撃が成功しないようにするため。
- C. 中間者攻撃が成功するのを防ぐため。
- D. ブルートフォース攻撃の成功を防ぐため。

正解: ([正解を表示します](#))

質問: 146

```
aaa new-model
radius-server host 10.0.0.12 key secret12
```

展示を参照してください。構成で使用される認証プロトコルに関する説明のうち正しいものはどれですか。

- A. 認証リクエストにはユーザー名のみが含まれます
- B. 認証および承認要求は1つのパケットにグループ化されます。
- C. 認証要求にはパスワードのみが含まれています
- D. 認証要求パケットと承認要求パケットが別々にあります。

正解: B ([コメントを发表する](#))

質問: 147

ユーザーは、複数のマシンからあまりにも多くの接続要求を受信しているネットワーク内のデバイスを持っています。デバイスはどのタイプの攻撃を受けていますか？

- A. フィッシング
- B. スローロリス
- C. SYNフラッド
- D. ファーミング

正解: ([正解を表示します](#))

質問: 148

エンジニアは、特定のOUIを持つエンドポイントを新しいエンドポイントグループに自動的に割り当てたいと考えています。このタイプのプロファイリングを機能させるには、どのプローブを有効にする必要がありますか？

- A. NetFlow

- B. NMAP
- C. SNMP
- D. DHCP

正解: ([正解を表示します](#))

Cisco ISEは、「プロファイリング」を実行することにより、ネットワークに接続しているデバイスまたはエンドポイントのタイプを判別できます。プロファイリングは、DHCP、SNMP、スパン、NetFlow、HTTP、RADIUS、DNS、またはNMAPスキャンを使用して行われ、デバイスのフィンガープリントを学習するために可能な限り多くのメタデータを収集します。NMAP（ネットワークマッパー）は、多くの機能を提供する人気のあるネットワークスキャナーです。それらの1つは、OUI（Organizationally Unique Identifier）情報です。OUIは、MACアドレスの最初の24ビットまたは6つの16進値です。注：DHCPプローブは、エンドポイントのOUIを収集できません。NMAPスキャンプローブは、次のエンドポイント属性を収集できます。+ EndPointPolicy + LastNmapScanCount + NmapScanCount + OUI +オペレーティングシステムリファレンス <http://www.network-node.com/blog/2016/1/2/ise-20-profiling> プロファイリングはDHCP、SNMP、スパン、NetFlow、HTTP、RADIUS、DNS、NMAP（ネットワークマッパー）は、多くの機能を提供する人気のあるネットワークスキャナーです。それらの1つは、OUI（Organizationally Unique Identifier）情報です。OUIは、MACアドレスの最初の24ビットまたは6つの16進値です。

注：DHCPプローブは、エンドポイントのOUIを収集できません。NMAPスキャンプローブは、次のエンドポイント属性を収集できます。

- + EndPointPolicy
- + LastNmapScanCount
- + NmapScanCount
- + OUI
- +オペレーティングシステム

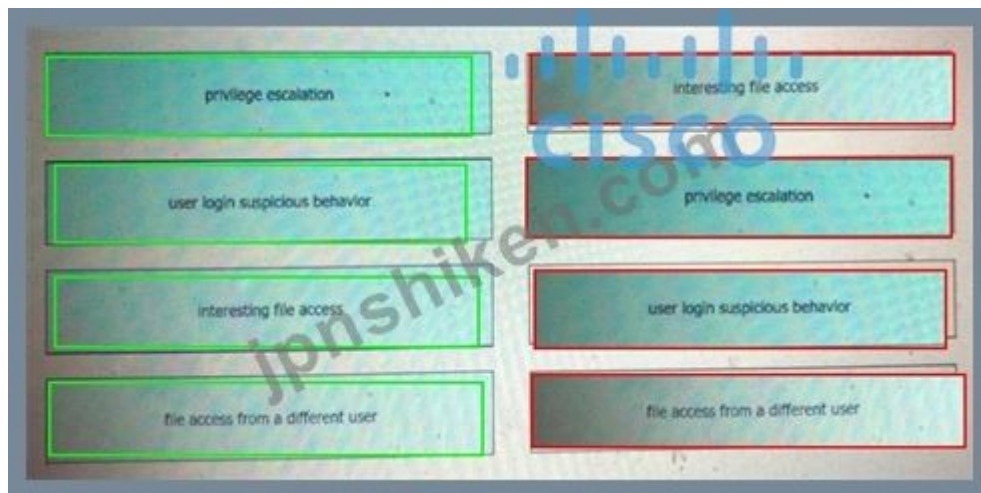
Cisco ISEは、「プロファイリング」を実行することにより、ネットワークに接続しているデバイスまたはエンドポイントのタイプを判別できます。プロファイリングは、DHCP、SNMP、スパン、NetFlow、HTTP、RADIUS、DNS、またはNMAPスキャンを使用して行われ、デバイスのフィンガープリントを学習するために可能な限り多くのメタデータを収集します。NMAP（ネットワークマッパー）は、多くの機能を提供する人気のあるネットワークスキャナーです。それらの1つは、OUI（Organizationally Unique Identifier）情報です。OUIは、MACアドレスの最初の24ビットまたは6つの16進値です。注：DHCPプローブは、エンドポイントのOUIを収集できません。NMAPスキャンプローブは次のエンドポイント属性を収集できます。+ EndPointPolicy + LastNmapScanCount + NmapScanCount + OUI +オペレーティングシステムリファレンス <http://www.network-node.com/blog/2016/1/2/ise-20-profiling>

質問: 149

Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。



正解:



質問: 150

Cisco ISEサーバとADドメインを統合する場合の前提条件は何ですか？

- A. Cisco ISEサーバとADサーバを同じサブネットに配置します
- B. 共通の管理者アカウントを構成する
- C. 共通のDNSサーバーを構成します
- D. Cisco ISEサーバとADサーバのクロックを同期します

正解: D ([コメントを发表する](#))

ActiveDirectoryをCisco ISEと統合するための前提条件は次のとおりです。

+ネットワークタイムプロトコル (NTP)サーバ設定を使用して、Cisco ISEサーバとActiveDirectory間の時刻を同期します。Cisco ISE CLIからNTP設定を設定できます。

+ Active Directory構造にマルチドメインフォレストがある場合、または複数のフォレストに分割されている場合は、Cisco ISEが接続されているドメインと、アクセスが必要なユーザおよびマシン情報を持つ他のドメインとの間に信頼関係が存在することを確認してください。信頼関係の確立の詳細については、Microsoft Active Directoryのドキュメントを参照してください。

+ Cisco ISEに参加しているドメインで、少なくとも1つのグローバルカタログサーバが動作可能であり、Cisco ISEからアクセスできる必要があります。ActiveDirectoryをCisco ISEと統合するための前提条件は次のとおりです。

+ネットワークタイムプロトコル (NTP)サーバ設定を使用して、CiscoISEサーバとActiveDirectory間の時刻を同期します。CiscoISECLIからNTP設定を設定できます。

+ Active Directory構造にマルチドメインフォレストがある場合、または複数のフォレストに分割されている場合は、Cisco ISEが接続されているドメインと、アクセスが必要なユーザおよびマシン情報を持つ他のドメインとの間に信頼関係が存在することを確認してください。信頼関係の確立の詳細については、MicrosoftActiveDirectoryのドキュメントを参照してください。

+ Cisco ISEに参加しているドメインで、少なくとも1つのグローバルカタログサーバが動作可能であり、CiscoISEからアクセスできる必要があります。参照：

b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24FActiveDirectoryをCiscoISEと統合するための前提条件は次のとおりです。

+ネットワークタイムプロトコル (NTP)サーバ設定を使用して、CiscoISEサーバとActiveDirectory間の時刻を同期します。CiscoISECLIからNTP設定を設定できます。

+ Active Directory構造にマルチドメインフォレストがある場合、または複数のフォレストに分割されている場合は、Cisco ISEが接続されているドメインと、アクセスが必要なユーザおよびマシン情報を持つ他のドメインとの間に信頼関係が存在することを確認してください。信頼関係の確立の詳細については、MicrosoftActiveDirectoryのドキュメントを参照してください。

+ Cisco ISEに参加しているドメインで、少なくとも1つのグローバルカタログサーバが動作可能であり、CiscoISEからアクセスできる必要があります。b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

質問: 151

VPNのセキュアハッシュアルゴリズムによって何が提供されますか？

- A. 認証
- B. 整合性
- C. 暗号化
- D. 鍵交換

正解: B ([コメントを発表する](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 152

ネットワーク管理者は、802.1X用のCiscoISEを使用するようにスイッチを設定しています。エンドポイントが認証に失敗しており、ネットワークにアクセスできません。管理者は、認証の詳細を確認するためにどこからトラブルシューティングを開始する必要がありますか？

- A. 適応型ネットワーク制御ポリシーリスト
- B. コンテキストの可視性
- C. 会計報告
- D. RADIUSライブログ

正解: ([正解を表示します](#))

ISEで失敗した認証と承認のトラブルシューティング方法

ISEライブログを確認してください

プライマリISEポリシー管理ノード (PAN)にログインします。

[操作]>[RADIUS]>[ライブログ]に移動します

オプション) イベントがRADIUSライブログに存在しない場合は、[操作]>[レポート]>[レポート]>[エンドポイントとユーザー]>[RADIUS認証]に移動し、ログで失敗した認証試行を確認します

質問: **153**

デバイスのコンプライアンスチェックに使用される2つのパラメータはどれですか？ 2つ選択してください。)

A. デバイスのオペレーティングシステムのバージョン

B. DNS整合性チェック

C. エンドポイント保護ソフトウェアバージョン

D. Windowsレジストリ値

E. DHCPスヌーピングチェック

正解: ([正解を表示します](#))

質問: **154**

Cisco Security Managerは何を管理していますか？

A. アクセスポイント

B. WSA

C. ASA

D. ESA

正解: ([正解を表示します](#))

Cisco Security Managerは、次の包括的な管理ソリューションを提供します。

-CiscoASA5500シリーズ適応型セキュリティアプライアンス

-シスコの侵入防止システム4200および4500シリーズセンサー

-CiscoAnyConnectセキュアモバイルティククライアント

Cisco Security Managerは、次の包括的な管理ソリューションを提供します。

-CiscoASA5500シリーズ適応型セキュリティアプライアンス

-シスコの侵入防止システム4200および4500シリーズセンサー

-CiscoAnyConnectセキュアモバイルティククライアント

Cisco Security Managerは、次の包括的な管理ソリューションを提供します。

-CiscoASA5500シリーズ適応型セキュリティアプライアンス

-シスコの侵入防止システム4200および4500シリーズセンサー

-CiscoAnyConnectセキュアモバイルティククライアント

質問: **155**

Cisco Next Generation Intrusion Prevention Systemで有効な抑制タイプはどれですか。 2つ選択してください)

A. アプリケーション

B. ルール

C. ポート

D. プロトコル

E. ソース

正解: B,E ([コメントを发表する](#))

質問: 156

Cisco WSAがWeb要求をチェックするとき、ユーザー定義のポリシーに一致できない場合はどうなりますか。

A. グローバルポリシーを適用します。

B. リクエストをブロックします。

C. 高度なポリシーを適用します。

D. 次の識別プロファイルポリシーを適用します。

正解: ([正解を表示します](#))

質問: 157

エンジニアは、ネットワーク上のトラフィックの中断に気づきます。さらに調査すると、ブロードキャストパケットがネットワークにフラッディングしていることがわかりました。この問題に対処するには、事前定義されたしきい値に基づいて何を構成する必要がありますか？

A. Bridge Protocol Data Unit Guard

B. 組み込みイベントの監視

C. アクセス制御リスト

D. ストームコントロール

正解: ([正解を表示します](#))

説明

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e1.html>

質問: 158

2つのDDoS攻撃カテゴリとは何ですか？ 2つ選択してください)

A. シーケンシャル

B. プロトコル

C. データベース

D. ボリュームベース

E. 画面ベース

正解: B,D ([コメントを发表する](#))

攻撃には3つの基本的なカテゴリがあります。+大量のトラフィックを使用してネットワーク帯域幅を氾濫させるボリュームベースの攻撃+サーバーリソースの悪用に焦点を当てたプロトコル攻撃+Webアプリケーションに焦点を当て、最も洗練された深刻な攻撃と見なされるアプリケーション攻撃攻撃の種類リファレンス <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

+大量のトラフィックを使用してネットワーク帯域幅を氾濫させるボリュームベースの攻撃

+サーバーリソースの悪用に焦点を当てたプロトコル攻撃

攻撃には3つの基本的なカテゴリがあります。+大量のトラフィックを使用してネットワーク帯域幅を氾濫させるボリュームベースの攻撃+サーバーリソースの悪用に焦点を当てたプロトコル攻撃+Webアプリケーションに焦点を当て、最も洗練された深刻な攻撃と見なされるアプリケーション攻撃攻撃の種類リファレンス <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

質問: 159

2つのルートキットタイプとは何ですか？ 2つ選択してください)

- A. 仮想
- B. ブートローダー
- C. レジストリ
- D. バッファモード
- E. ユーザーモード

正解: [\(正解を表示します\)](#)

質問: 160

ユーザーがオンプレミスのESAソリューションとCESソリューションを選択するのはなぜですか？

- A. 需要は予測できません。
- B. 機密データはオンサイトに残しておく必要があります。
- C. サーバーチームはこのサービスを外部委託したいと考えています。
- D. ESAはインラインで展開されます。

正解: D ([コメントを發表する](#))

質問: 161

アプリケーションで月次または四半期ごとではなく、週次または日次の更新を提供するDevSecOps実装プロセスはどれですか？

- A. オーケストレーション
- B. CI/CDパイプライン
- C. コンテナ
- D. セキュリティ

正解: B ([コメントを發表する](#))

従来のソフトウェアライフサイクルとは異なり、CI / CD実装プロセスでは、月次または四半期ごとではなく、週次または日次の更新が行われます。楽しい部分は、顧客がその場で行われるため、更新がアプリケーションにあることに気付かないことです。

従来のソフトウェアライフサイクルとは異なり、CI / CD実装プロセスでは、月次または四半期ごとではなく、週次または日次の更新が行われます。楽しい部分は、顧客がその場で行われるため、更新がアプリケーションにあることに気付かないことです。

参照：

従来のソフトウェアライフサイクルとは異なり、CI / CD実装プロセスでは、月次または四半期ごとではなく、週次または日次の更新が行われます。楽しい部分は、顧客がその場で行われるため、更新がアプリケーションにあることに気付かないことです。

質問: 162

802.1x展開でMAB要求をフィルタリングするために使用できるRADIUS属性はどれですか。

- A. 1
- B. 6
- C. 2
- D. 31

正解: B ([コメントを發表する](#))

質問: 163

IPsecのステートフルフェールオーバーの前提条件となる2つの条件はどれですか。(2つ選択してください。)

- A. アクティブデバイスに設定されているIKE構成のみを、スタンバイデバイスに複製する必要があります。IPsec構成が自動的にコピーされます。
- B. アクティブデバイスとスタンバイデバイスは、異なるバージョンのCisco IOSソフトウェアを実行できますが、同じタイプのデバイスである必要があります。
- C. アクティブデバイスで設定されているIPsec構成のみを、スタンバイデバイスで複製する必要があります。IKE構成は自動的にコピーされます。
- D. アクティブデバイスとスタンバイデバイスは、同じバージョンのCisco IOSソフトウェアを実行し、同じタイプのデバイスである必要があります。
- E. アクティブデバイスで設定されているIPsec構成は、スタンバイデバイスで複製する必要があります。

正解: ([正解を表示します](#))

質問: 164

Cisco DNA Centerの2つの機能のうち、ソフトウェア定義ネットワークソリューションで使用されているものはどれですか。(2つ選択してください。)

- A. 会計
- B. 保証
- C. 自動化
- D. 認証
- E. 暗号化

正解: ([正解を表示します](#))

説明/リファレンス <https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html>

質問: 165

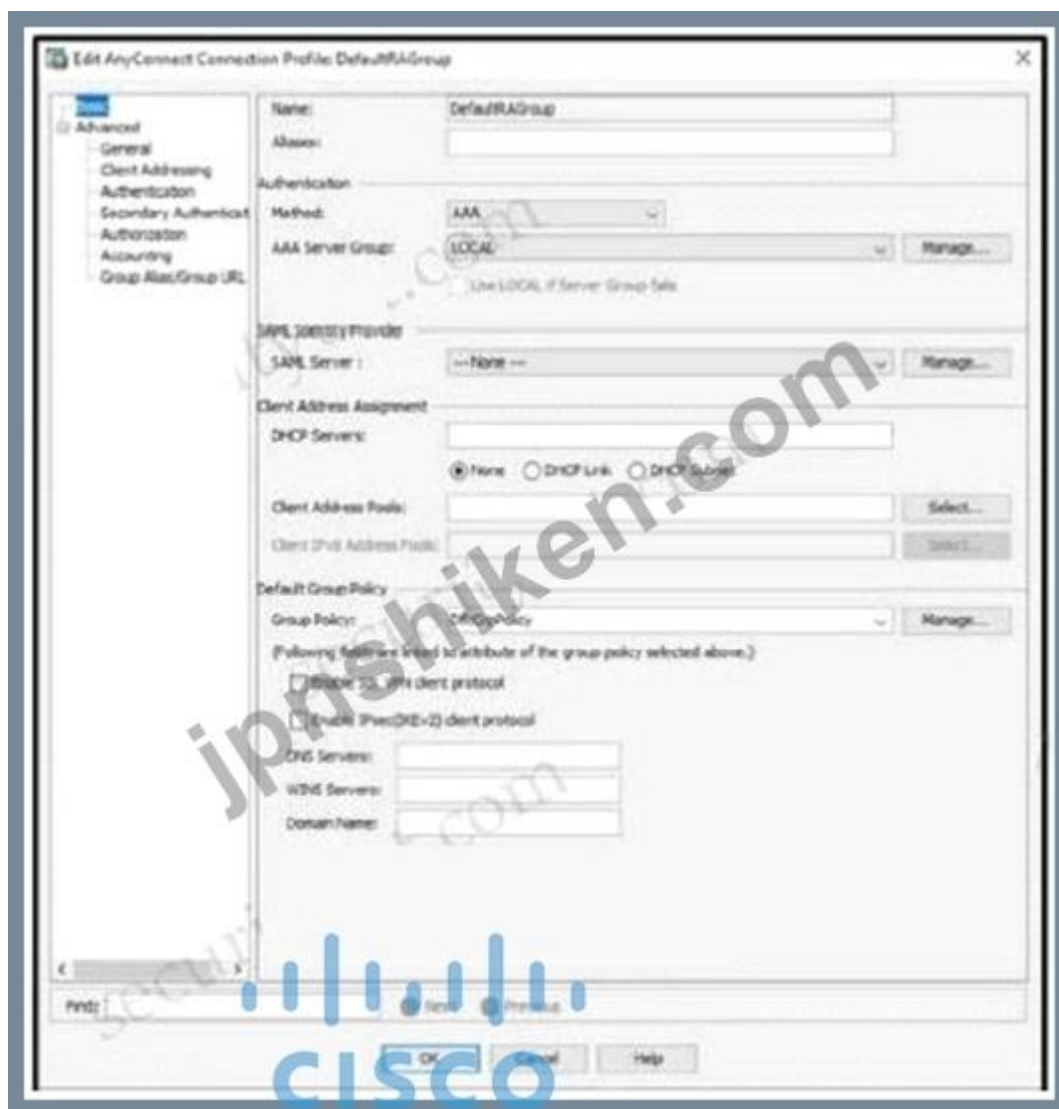
エンジニアがエンドポイント用にAMPを構成していて、特定のファイルの実行をブロックしたいと考えています。このタスクを実行するために使用されるアウトブレイク制御方法はどれですか？

- A. 簡単な検出
- B. デバイスフローの相関
- C. アプリケーションブロックリスト
- D. 高度なカスタム検出

正解: ([正解を表示します](#))

質問: 166

展示を参照してください。



Cisco ASAで終端するリモートアクセスVPNソリューションを設定する場合、管理者は、マシン証明書を使用したAAA認証と組み合わせて外部トークン認証メカニズムを利用したいと考えています。これを可能にするには、どの構成アイテムを変更する必要がありますか？

- A. グループポリシー
- B. 方法
- C. SAMLサーバー
- D. DHCPサーバー

正解: [\(正解を表示します\)](#)

AAAを外部トークン認証メカニズムと一緒に使用するには、認証で「メソッド」を「両方」に設定します。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

エンジニアは、転送中のデータの保護を追加し、電子メールメッセージにヘッダーを含める必要があります。この目標を達成するには、どの構成が必要ですか。

- A. メールアプライアンスをプロビジョニングします
- B. フラグ付きメッセージ処理を有効にする
- C. 送信者の！Pアドレスをホストインターフェイスにマップします。
- D. 暗号化アプライアンスを展開します。

正解: [\(正解を表示します\)](#)

質問: 168

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

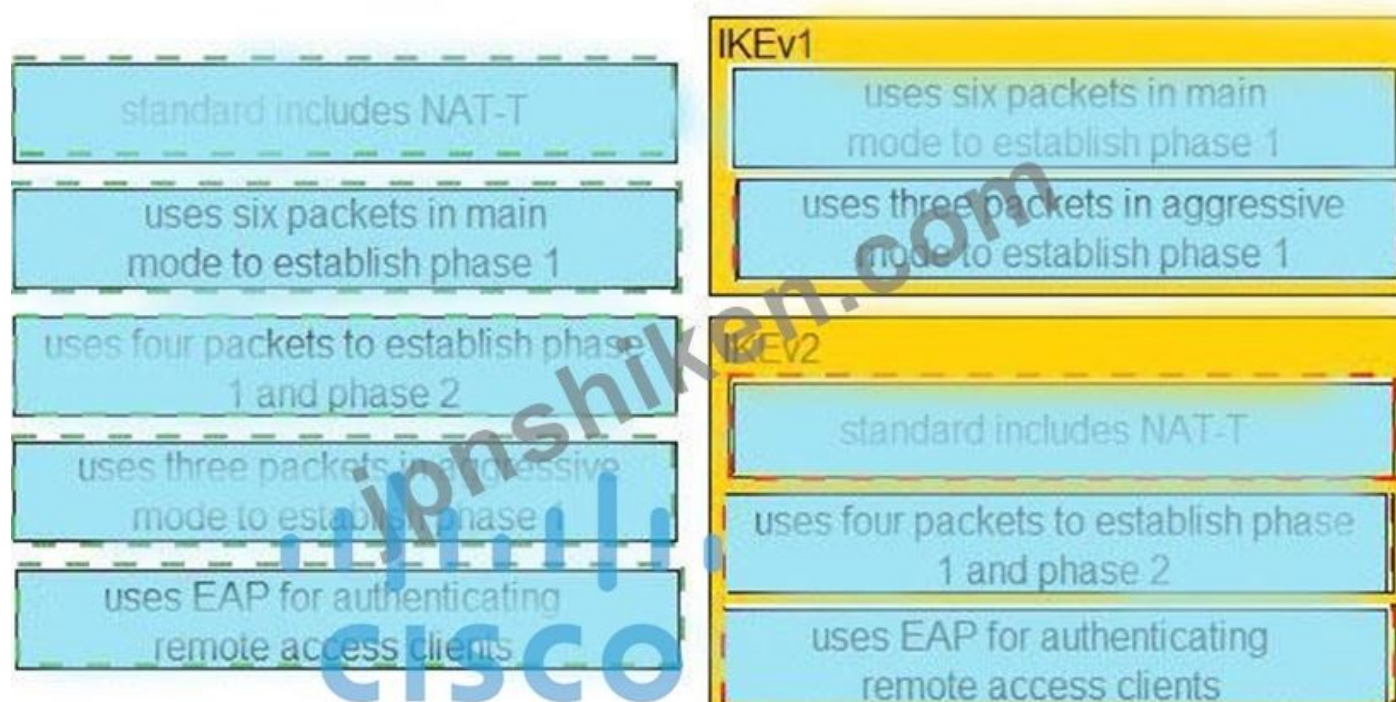
uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

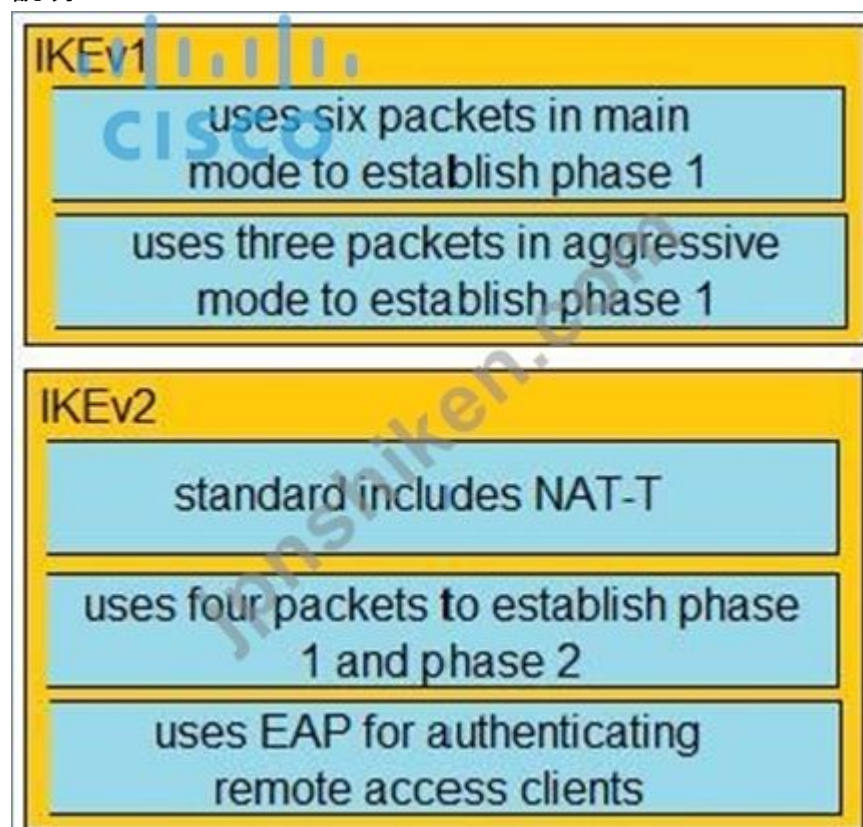
IKEv1

IKEv2

正解:



説明



質問: 169

URLカテゴリを使用したアクセスコントロールをサポートするCiscoWSA機能はどれですか。

- A. Web使用制御
- B. SOCKSプロキシサービス
- C. ユーザーセッションの制限
- D. 透過的なユーザーID

正解: ([正解を表示します](#))

質問: 170

Cisco ISE環境でのマイデバイスポータル目的は何ですか。

- A. エンドユーザーが所有するシステムでウイルス対策の定義とパッチを管理および展開する
- B. 新しいラップトップとモバイルデバイスを登録する
- C. ユーザーレスおよびエージェントレスシステムをプロビジョニングする
- D. 新しくプロビジョニングされたモバイルデバイスをリクエストする

正解: ([正解を表示します](#))

Employees can use the My Devices portal to register and manage their personal devices. The My Devices portal includes online help that provides

質問: 171

RSAキーがエクスポートおよびインポートされる時に、どのタイプの保護がRSAキーを暗号化しますか？

- A. エクスポート不可
- B. NGE
- C. パスフレーズ
- D. ファイル

正解: ([正解を表示します](#))

質問: 172

Cisco DNA Center APIの2つの特徴は何ですか？ 2つ選択してください

- A. ネットワークの全体的な状態を表示します
- B. これらはシスコ独自のものです。
- C. Pythonスクリプトをサポートしていません。
- D. 新しいデバイスをすばやくプロビジョニングします。
- E. Cisco DNA Center API呼び出しを利用するには、Postmanが必要です。

正解: A,D ([コメントを发表する](#))

質問: 173

PACファイルを使用したWSAHTTPプロキシ構成に関する2つの事実は何ですか？ 2つ選択してください。）

- A. ブリッジプロキシ展開として定義されています。
- B. プロキシを参照するPACファイルは、クライアントのWebブラウザーにデプロイされます。
- C. 透過プロキシ展開として定義されています。
- D. 明示的なプロキシ展開として定義されています。
- E. デュアルNIC構成では、PACファイルは2つのNICを介してトラフィックをプロキシに転送します。

正解: ([正解を表示します](#))

質問: 174

ユーザーは、複数のマシンからあまりにも多くの接続要求を受信しているネットワーク内のデバイスを持っています。デバイスはどのタイプの攻撃を受けていますか？

- A. SYNフラッド
- B. スローロリス
- C. ファーミング
- D. フィッシング

正解: [\(正解を表示します\)](#)

説明

<https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html#~types-of-ddos-attacks>

質問: 175

ステップを左から右の正しい順序にドラッグアンドドロップして、AppDynamicsがアマゾンウェブサービスのEC2インスタンスを監視できるようにします。

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

正解:

Install monitoring extension for AWS EC2.	Configure a Machine Agent or SIM Agent.
Restart the Machine Agent.	Install monitoring extension for AWS EC2.
Update config.yaml.	Update config.yaml.
Configure a Machine Agent or SIM Agent.	Restart the Machine Agent.

Configure a Machine Agent or SIM Agent.

Install monitoring extension for AWS EC2.

Update config.yaml.

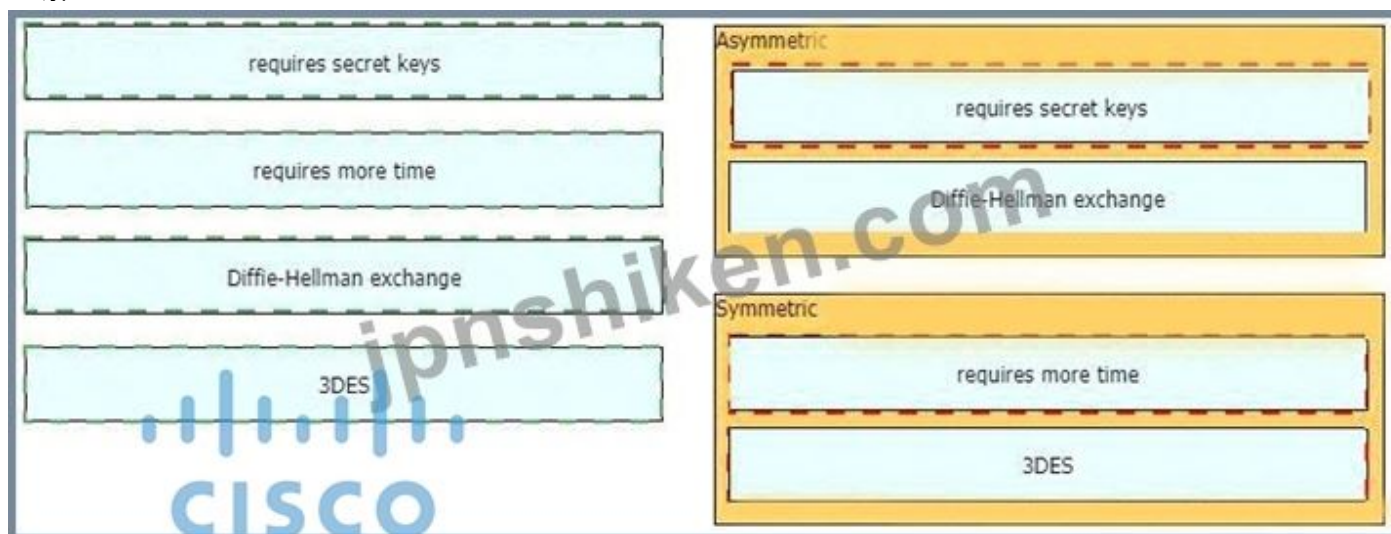
Restart the Machine Agent.

質問: 176

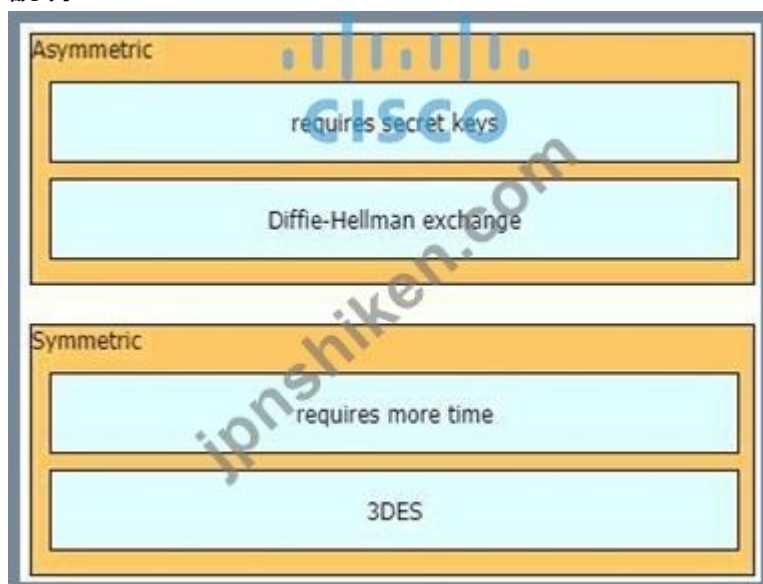
説明を左側から右側の暗号化アルゴリズムにドラッグアンドドロップします。



正解:



説明



質問: 177

パケットTTL、IP / TCPフラグ、ペイロード長など、フロー内で見られる変動をキャプチャするテレメトリデータはどれですか？

- A. パケット間バリエーション
- B. ソフトウェアパッケージのバリエーション

C. フローインサイトのバリエーション

D. プロセスの詳細のバリエーション

正解: **A** ([コメントを发表する](#))

テレメトリ情報は、次の3種類のデータで構成されています。

+フロー情報 :この情報には、エンドポイント、プロトコル、ポート、フローが開始された日時、フローがアクティブだった期間などに関する詳細が含まれます。

+パケット間変動 :この情報は、フロー内のパケット間変動をキャプチャします。例には、存続時間 (TTL)、IPおよびTCPフラグ、ペイロード長などの変動が含まれます

+コンテキストの詳細 :コンテキスト情報は、パケットヘッダーの外部で取得されます。これには、バッファ使用率の変動、フロー内のパケットドロップ、トンネルエンドポイントとの関連付けなどに関する詳細が含まれます。

テレメトリ情報は、次の3種類のデータで構成されています。

+フロー情報 :この情報には、エンドポイント、プロトコル、ポート、フローが開始された日時、フローがアクティブだった期間などに関する詳細が含まれます。

+パケット間変動 :この情報は、フロー内のパケット間変動をキャプチャします。例には、存続時間 (TTL)、IPおよびTCPフラグ、ペイロード長などの変動が含まれます

+コンテキストの詳細 :コンテキスト情報は、パケットヘッダーの外部で取得されます。これには、バッファ使用率の変動、フロー内のパケットドロップ、トンネルエンドポイントとの関連付けなどに関する詳細が含まれます。

参照 :

[cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf](#)

テレメトリ情報は、次の3種類のデータで構成されています。

+フロー情報 :この情報には、エンドポイント、プロトコル、ポート、フローが開始された日時、フローがアクティブだった期間などに関する詳細が含まれます。

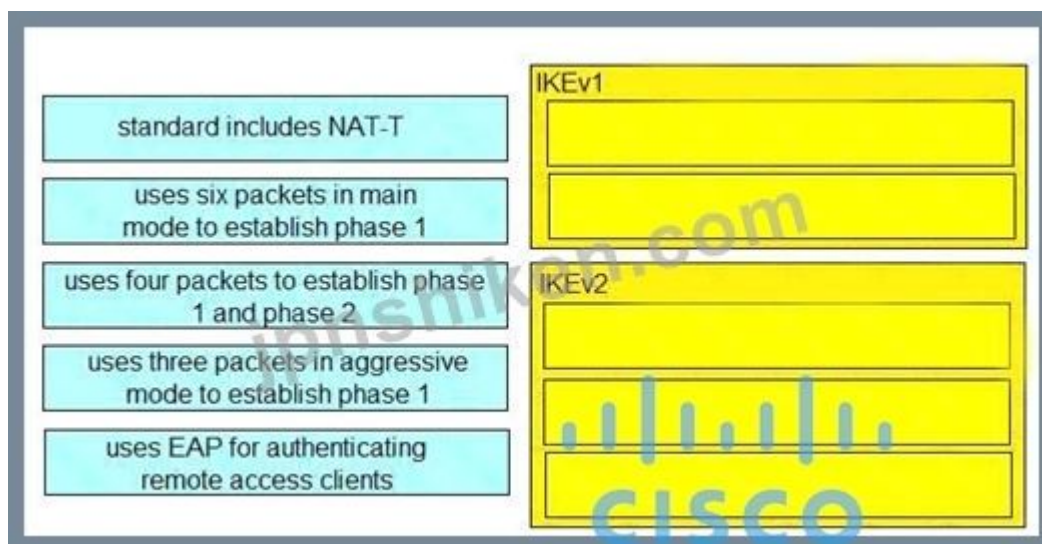
+パケット間変動 :この情報は、フロー内のパケット間変動をキャプチャします。例には、存続時間 (TTL)、IPおよびTCPフラグ、ペイロード長などの変動が含まれます

+コンテキストの詳細 :コンテキスト情報は、パケットヘッダーの外部で取得されます。これには、バッファ使用率の変動、フロー内のパケットドロップ、トンネルエンドポイントとの関連付けなどに関する詳細が含まれます。

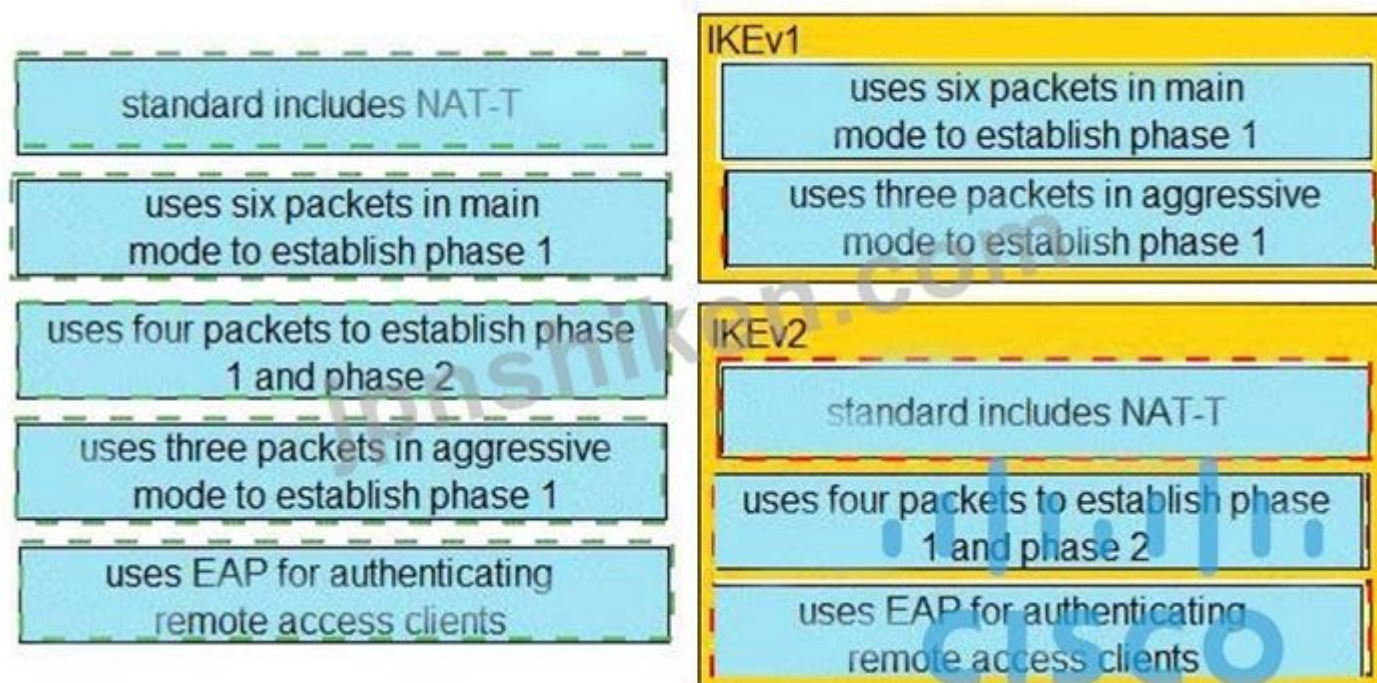
[cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf](#)

質問: **178**

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。



正解:



説明

IKEv1	uses six packets in main mode to establish phase 1
	uses three packets in aggressive mode to establish phase 1
IKEv2	standard includes NAT-T
	uses four packets to establish phase 1 and phase 2
	uses EAP for authenticating remote access clients

質問: 179

Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。

privilege escalation	Tetration platform learns the normal behavior of users.
user login suspicious behavior	Tetration platform is armed to look at sensitive files.
interesting file access	Tetration platform watches user access failures and methods.
file access from a different user	Tetration platform watches for movement in the process lineage tree.

正解:



質問: 180

CおよびC++プログラミング言語に一般的に関連する攻撃はどれですか？

- A. クロスサイトスクリプティング
- B. ウォーターホール
- C. DDoS
- D. バッファオーバーフロー

正解: D ([コメントを发表する](#))

説明

バッファオーバーフロー (またはバッファオーバーラン)は、データの量がメモリバッファのストレージ容量を超えると発生します。その結果、バッファにデータを書き込もうとするプログラムは、隣接するメモリ位置を上書きします。

バッファオーバーフローは、CおよびC++の低レベルコードの脆弱性です。攻撃者は、プログラムをクラッシュさせたり、データを破損させたり、個人情報盗んだり、自分のコードを実行したりする可能性があります。これは基本的に、割り当てられたメモリスペース外のバッファにアクセスすることを意味します。これは、アレイの場合に非常に頻繁に発生します。

質問: 181

CoAがデバイスでサポートされるように、認証、許可、およびアカウンティングをグローバルに有効にするCiscoコマンドはどれですか。

- A. ip device-tracking
- B. auth-type all
- C. aaa server radius dynamic-author
- D. aaa new-model

正解: ([正解を表示します](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **182**

アプリケーションの可視性とセグメンテーションにより、ハイブリッドクラウド展開のワークロードを保護するソリューションはどれですか？

- A. ネクサス
- B. ステルスウォッチ
- C. 火力
- D. テトレーション

正解: ([正解を表示します](#))

説明/リファレンス <https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/index.html#~products>

質問: **183**

Cisco AnyConnect VPNを使用するときに、最も強力なスループットパフォーマンスを提供するプロトコルはどれですか。

- A. TLSv1.2
- B. TLSv1.1
- C. BJTLSv1
- D. DTLSv1

正解: ([正解を表示します](#))

DTLSはUDPベースであるため、遅延に敏感なアプリケーション（音声およびビデオ）に使用されますが、TLSはTCPベースです。したがって、DTLSは最強のスループットパフォーマンスを提供します。AnyConnect接続時のDTLSのスループットは、VPNスループットに近い処理パフォーマンスが期待できます。

質問: **184**

Cisco ISEサーバとADドメインを統合する場合の前提条件は何ですか？

- A. Cisco ISEサーバとADサーバを同じサブネットに配置します
- B. 共通の管理者アカウントを構成する
- C. 共通のDNSサーバーを構成します
- D. Cisco ISEサーバとADサーバのクロックを同期します

正解: **D** ([コメントを發表する](#))

ActiveDirectoryをCisco ISEと統合するための前提条件は次のとおりです。

+ ネットワークタイムプロトコル (NTP) サーバ設定を使用して、Cisco ISEサーバとActiveDirectory間の時刻を同期します。Cisco ISE CLIからNTP設定を設定できます。

+ Active Directory構造にマルチドメインフォレストがある場合、または複数のフォレストに分割されている場合は、Cisco ISEが接続されているドメインと、アクセスが必要なユーザおよびマシン情報を持つ他のドメインとの間に信頼関係が存在することを確認してください。信頼関係の確立の詳細については、Microsoft ActiveDirectoryのドキュメントを参照してください。

+ Cisco ISEに参加しているドメインで、少なくとも1つのグローバルカタログサーバが動作可能であり、Cisco ISEからアクセスできる必要があります。ActiveDirectoryをCisco ISEと統合するための前提条件は次のとおりです。

+ネットワークタイムプロトコル (NTP)サーバ設定を使用して、Cisco ISEサーバとActiveDirectory間の時刻を同期します。Cisco ISE CLIからNTP設定を設定できます。

+ Active Directory構造にマルチドメインフォレストがある場合、または複数のフォレストに分割されている場合は、Cisco ISEが接続されているドメインと、アクセスが必要なユーザおよびマシン情報を持つ他のドメインとの間に信頼関係が存在することを確認してください。信頼関係の確立の詳細については、Microsoft Active Directoryのドキュメントを参照してください。

+ Cisco ISEに参加しているドメインで、少なくとも1つのグローバルカタログサーバが動作可能であり、Cisco ISEからアクセスできる必要があります。Active DirectoryをCisco ISEと統合するための前提条件は次のとおりです。

+ネットワークタイムプロトコル (NTP)サーバ設定を使用して、Cisco ISEサーバとActiveDirectory間の時刻を同期します。Cisco ISE CLIからNTP設定を設定できます。

+ Active Directory構造にマルチドメインフォレストがある場合、または複数のフォレストに分割されている場合は、Cisco ISEが接続されているドメインと、アクセスが必要なユーザおよびマシン情報を持つ他のドメインとの間に信頼関係が存在することを確認してください。信頼関係の確立の詳細については、Microsoft Active Directoryのドキュメントを参照してください。

+ Cisco ISEに参加しているドメインで、少なくとも1つのグローバルカタログサーバが動作可能であり、Cisco ISEからアクセスできる必要があります。参照：

b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

質問: 185

構成されたポスチャポリシー要件が満たされていない場合、どのコンプライアンスステータスが表示されますか？

- A. 準拠
- B. 不明
- C. 承認済み
- D. 非準拠

正解: (正解を表示します)

ポスチャは、Cisco Identity Services Engine (Cisco ISE)のサービスであり、企業のセキュリティポリシーに準拠しているかどうか、ネットワークに接続しているすべてのエンドポイントの状態 (ポスチャとも呼ばれます)を確認できます。ポスチャポリシーは、1つ以上のIDグループおよびオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。+必須要件が失敗した場合、ユーザーは非準拠状態に移行します+オプション要件が失敗した場合、ユーザーは指定されたオプション要件をスキップでき、ユーザーは準拠状態に移行しますこのQdidはタイプを明確に指定していませんポスチャポリシー要件 (必須またはオプション)が満たされていないため、ユーザーは非準拠または準拠状態になる可能性があります。だが "

ポスチャポリシーは、1つ以上のIDグループおよびオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。

ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。

+必須要件が満たされない場合、ユーザーは非準拠状態に移行します

+オプションの要件が失敗した場合、ユーザーは指定されたオプションの要件をスキップでき、ユーザーは準拠状態に移行します。このQdidは、姿勢ポリシー要件のタイプ (必須またはオプション)が満たされていないため、ユーザーは非準拠または準拠状態。ただし、ここでは「非準拠」が最善の答えです。

参照：

ポスチャは、Cisco Identity Services Engine (Cisco ISE)のサービスであり、企業のセキュリティポリシーに準拠しているかどうか、ネットワークに接続しているすべてのエンドポイントの状態 (ポスチャとも呼ばれます)を確認できます。ポスチャポリシーは、1つ以上のIDグループおよびオペレーティン

グシステムに関連付けられているポスチャ要件のコレクションです。ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。+必須要件が失敗した場合、ユーザーは非準拠状態に移行します+オプション要件が失敗した場合、ユーザーは指定されたオプション要件をスキップでき、ユーザーは準拠状態に移行しますこのQdidはタイプを明確に指定していませんポスチャポリシー要件（必須またはオプション）が満たされていないため、ユーザーは非準拠または準拠状態になる可能性があります。だが "

質問: 186

TAXIIがサポートする2つの機能はどれですか？ 2つ選択してください)

- A. 交換
- B. プルメッセージング
- C. バインディング
- D. 相関
- E. 軽減

正解: B,C ([コメントを发表する](#))

説明

Trusted Automated eXchange of Indicator Information (TAXII)は、ネットワークを介して当事者間で構造化されたサイバー脅威情報を交換するためのメカニズムを指定します。

TAXIIは、構造化されたサイバー脅威情報の共有に関心のある人々に特定の機能を提供するために存在します。

TAXII機能は、TAXIIアクションを記述できる最高レベルです。このバージョンのTAXIIがサポートする機能には、プッシュメッセージング、プルメッセージング、および検出の3つがあります。

リストには「バインド」機能はありませんが、ここでの最良の答えです。

質問: 187

エンジニアは、LDAPがリスナーでクエリを受け入れることを有効にしました。悪意のある攻撃者がすべての有効な受信者をすばやく特定できないようにする必要があります。この目標を達成するには、Cisco ESAで何をする必要がありますか？

- A. バウンス検証を使用する
- B. 着信コンテンツフィルターを構成します。
- C. 受信者アクセステーブルのLDAPアクセスクエリをバイパスします。
- D. ディレクトリハーベスト攻撃防止を構成する

正解: ([正解を表示します](#))

説明

How do you create an LDAP group query on the ESA?

1. Create an LDAP group query under System Administration > LDAP.
2. Enable the group query for the listener under Network > Listener > {select the listener} > select the LDAP group query.
3. Go to Incoming Mail Policies.
4. Create a new policy for the group.
5. Add in the recipient matching the group.
6. Choose LDAP group query instead of email.
7. Select group query and put in the matching group name.
8. **Configure new incoming mail policies:** Anti-Spam, Anti-Virus, Content Filters, and Virus Outbreak Filters.

質問: 188

Ciscoスイッチで802.1Xをグローバルに有効にするコマンドはどれですか。

- A. aaa new-model
- B. dot1xpaeオーセンティケーター
- C. dot1x system-auth-control
- D. 認証ポート制御自動

正解: [\(正解を表示します\)](#)

質問: 189

Cisco ASA Netflowの機能は何ですか？

- A. すべてのイベントタイプを同じコレクターにのみログに記録します。
- B. トラフィックに基づいてNSELイベントをフィルタリングします。
- C. MPFが設定されていない場合でもNSELイベントを生成します。
- D. アクティブスタンバイフェールオーバーペアのアクティブASAとスタンバイASAからNetFlowデータレコードを送信します。

正解: B [\(コメントを発表する\)](#)

質問: 190

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:



質問: 191

透過モードで実行されているCiscoWSAと明示モードで実行されているCiscoWSAの2つの違いは何ですか。(2つ選択してください。)

- A. Cisco WSAが透過モードで実行されている場合、HTTP要求の宛先としてWSA自身のIPアドレスを使用します。
- B. Cisco WSAは、明示モードで実行されている場合にのみ、独自のIPアドレスで応答します。
- C. Cisco WSAは、透過モードで実行されている場合にのみ、独自のIPアドレスで応答します。
- D. Cisco WSAは、透過モードで実行されている場合にのみWebブラウザで設定されます。
- E. Cisco WSAは、透過モードで実行されている場合にのみ、レイヤ3デバイスを使用してトラフィックをリダイレクトします。

正解: ([正解を表示します](#))

質問: 192

Cisco DNA Centerの2つの機能のうち、ソフトウェア定義ネットワークソリューションで使用されているものはどれですか。(2つ選択してください。)

- A. 自動化
- B. 保証
- C. 認証
- D. 暗号化
- E. 会計

正解: ([正解を表示します](#))

質問: 193

Cisco ESA管理者は、隔離された電子メールが配信される前にウイルスがないことを確認するようにCiscoESAを設定する必要があります。さらに、既知の不良メールサーバーからのメールの配信を防止する必要があります。これらの要件を満たすために実行する必要がある2つのアクションはどれですか？ (2つ選択してください)

- A. SenderBaseのアウトブレイクフィルターを使用する
- B. メッセージ追跡サービスを有効にする
- C. 受信者アクセステーブルを設定します
- D. CiscoESAをDMZに導入します
- E. アンチウイルス署名を使用して隔離された電子メールをスキャンする

正解: **A,E** ([コメントを发表する](#))

説明説明ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。参照 https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、注 :リモートアクセストロイの木馬 (RAT)と混同しないように、受信者アクセステーブル (RAT)は、どの受信者が一般に受け入れられるかを定義するCiscoESA用語です。リスナー。

説明

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

参照 :

[b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html](https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html)

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

説明説明ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。参照 https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、注 :リモートアクセストロイの木馬 (RAT)と混同しないように、受信者アクセステーブル (RAT)は、どの受信者が一般に受け入れられるかを定義するCiscoESA用語です。リスナー。

質問: **194**

crypto isakmp key ciscXXXXXXXX address 172.16.0.0コマンドを実行した結果はどうなりますか？

A. キーciscXXXXXXXXを使用して、172.16.0.0/16の範囲のIKEv2ピアを認証します

- B. キーciscXXXXXXXXXを使用して、172.16.0.0/32ピアのIPアドレスを認証します
- C. キーciscXXXXXXXXXを使用して、172.16.0.0/16の範囲のIKEv1ピアを認証します
- D. キーciscXXXXXXXXXを使用して、IKEExchange内のすべての証明書を保護します

正解: ([正解を表示します](#))

説明/リファレンス <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000>

質問: 195

展示を参照してください。

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'
api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

Ciscoセキュリティアプライアンスに接続すると、APIは何をしますか？

- A. AMPを管理するためのSNMPプルメカニズムを作成します
- B. ネットワーク内のコンピューターからプロセスとPID情報を取得します
- C. エンドポイントのAMPからネットワークテレメトリ情報を収集します
- D. AMPが認識しているコンピューターに関するネットワークインターフェイス情報を収集します

正解: ([正解を表示します](#))

質問: 196

Firepower Next Generation Intrusion Prevention System検出器を、左側から右側の正しい定義にドラッグアンドドロップします。

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

正解:

PortScan Detection	Distributed PortScan
Port Sweep	Decoy PortScan
Decoy PortScan	Port Sweep
Distributed PortScan	PortScan Detection

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 197

CiscoASA用のCiscoNetFlowセキュアイベントロギングの機能は何ですか。

- A. 複数のNetFlowコレクターがサポートされています
- B. 高度なNetFlowv9テンプレートとレガシーv5フォーマットがサポートされています
- C. セキュアNetFlow接続はCiscoPrimeInfrastructure用に最適化されています
- D. フロー作成イベントが遅延します

正解: D (コメントを发表する)

NetFlow Secure Event Logging (NSEL)のASAおよびASASM実装は、次の主要な機能を提供します。

..。

-フロー作成イベントのエクスポートを遅らせます。

NetFlow Secure Event Logging (NSEL)のASAおよびASASM実装は、次の主要な機能を提供します。

..。

-フロー作成イベントのエクスポートを遅らせます。

NetFlow Secure Event Logging (NSEL)のASAおよびASASM実装は、次の主要な機能を提供します。

..。

-フロー作成イベントのエクスポートを遅らせます。

質問: 198

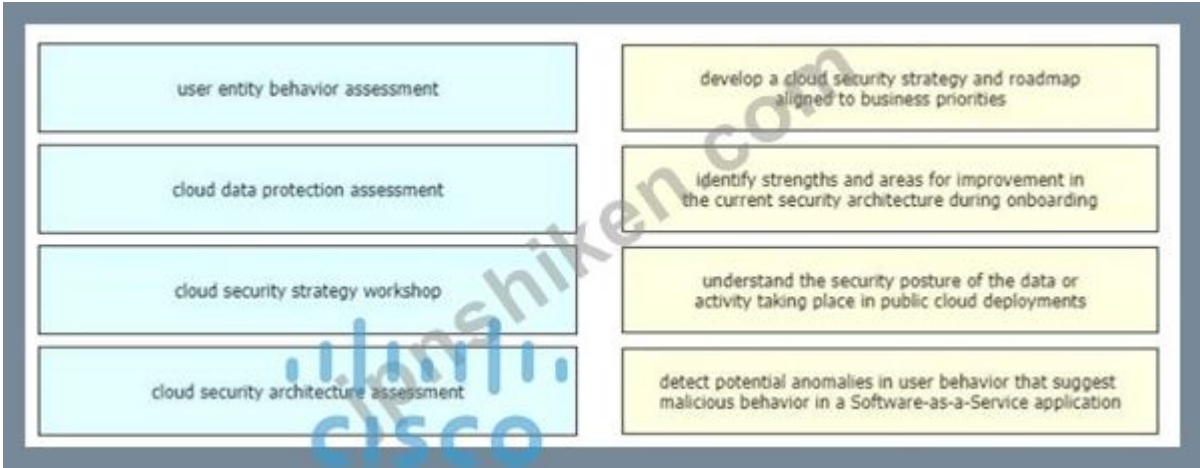
テナントが仮想マシンOSのパッチ適用を担当するクラウドサービスモデルはどれですか？

- A. UCaaS
- B. PaaS
- C. IaaS
- D. SaaS

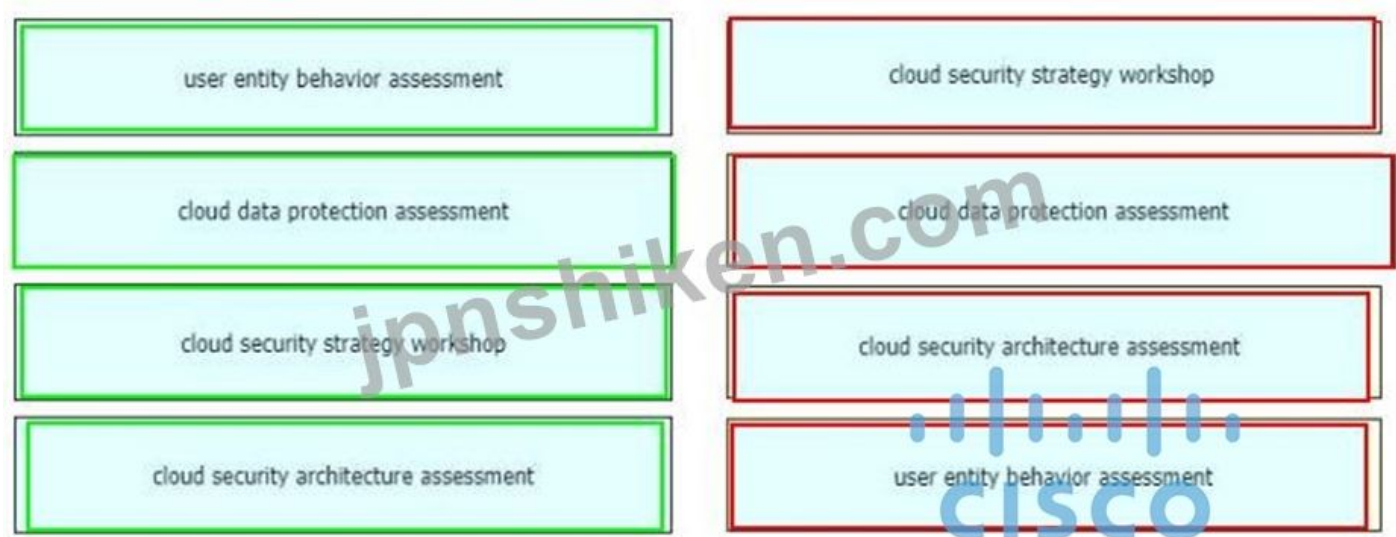
正解: [\(正解を表示します\)](#)

質問: 199

クラウドセキュリティ評価コンポーネントを左側から右側の定義にドラッグアンドドロップします。



正解:



質問: 200

攻撃者は、DNS要求およびクエリ内のデータを非表示にしてエンコードするために、どの抽出方法を使用しますか？

- A. DNSトンネリング
- B. DNSCrypt
- C. DNSセキュリティ

D. DNSSEC

正解: [\(正解を表示します\)](#)

説明

DNSトンネリングは、DNSクエリおよび応答で他のプログラムまたはプロトコルのデータをエンコードするサイバー攻撃の方法です。DNSトンネリングには、攻撃されたDNSサーバーに追加され、リモートサーバーとアプリケーションを制御するために使用されるデータペイロードが含まれることがよくあります。

質問: 201

エンドポイント保護プラットフォームではなく、エンドポイント検出および応答ソリューションを選択する必要があるのはどのような状況ですか？

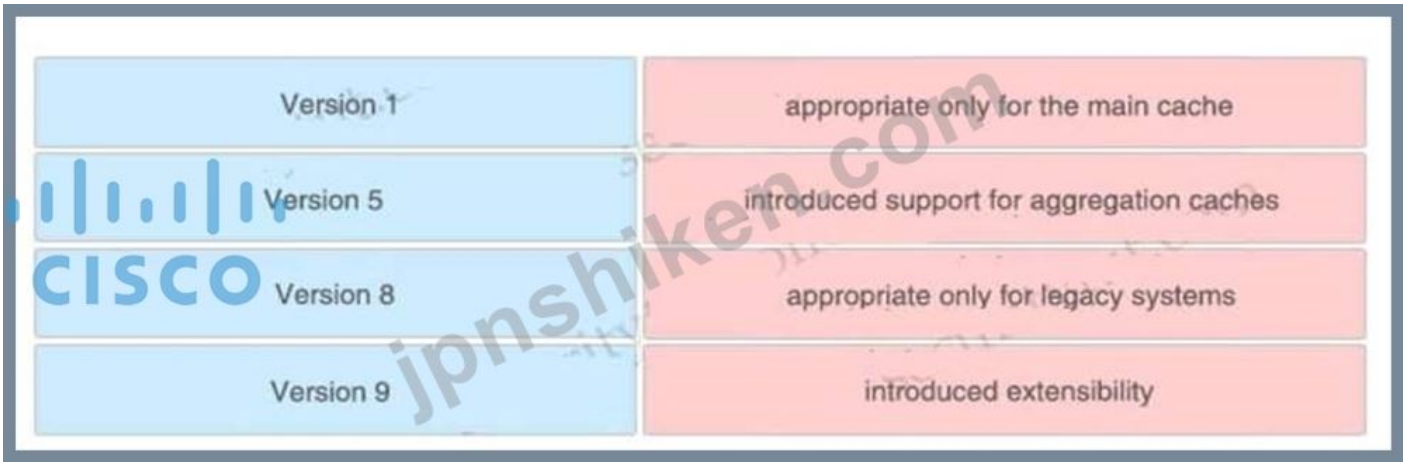
- A. 従来のマルウェア対策検出が必要な場合
- B. ソリューションを一元管理する必要がない場合
- C. ネットワーク上にファイアウォールがない場合
- D. より高度な検出機能が必要な場合

正解: [\(正解を表示します\)](#)

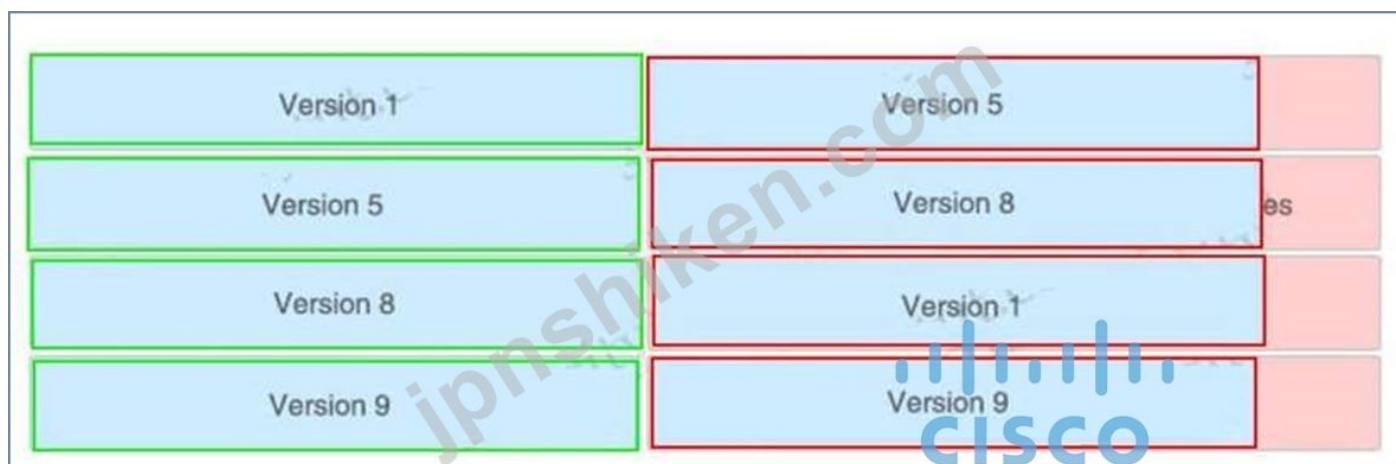
エンドポイント保護プラットフォーム (EPP)は、既知および未知のマルウェアなどのエンドポイントセキュリティの脅威を防ぎます。エンドポイント検出および応答 (EDR)ソリューションは、EPPやその他のセキュリティツールが検出できなかった脅威を検出して応答できます。EDRとEPPの目標は似ていますが、異なる目的を達成するように設計されています。EPPは、悪意のあるファイルを識別し、潜在的に悪意のあるアクティビティを検出し、インシデントの調査と対応のためのツールを提供することにより、デバイスレベルの保護を提供するように設計されています。EPPの予防的性質は、予防的EDRを補完します。EPPは防御の最前線として機能し、組織の展開されたセキュリティソリューションによって検出される可能性のある攻撃を除外します。EDRは、保護の第2層として機能し、セキュリティアナリストが脅威ハンティングを実行し、エンドポイントに対するより微妙な脅威を特定できるようにします。効果的なエンドポイント防御には、EDRとEPPの両方の機能を統合して、組織のセキュリティチームを圧倒することなくサイバー脅威に対する保護を提供するソリューションが必要です。

質問: 202

NetFlowエクスポートフォーマットを左から右の説明にドラッグアンドドロップします。



正解:



質問: 203

Cisco Security Managerは何を管理していますか？

- A. WSA
- B. ASA
- C. アクセスポイントO
- D. ESA

正解: B ([コメントを发表する](#))

参照：

<https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html>

質問: 204

企業は、オンプレミスに保存されていないクレジットカード番号の流出を経験しています。会社は、環境全体で機密データを保護できる必要があります。この目標を達成するには、どのツールを使用する必要がありますか？

- A. セキュリティマネージャー
- B. クラウドロック
- C. Webセキュリティアプライアンス
- D. Cisco ISE

正解: ([正解を表示します](#))

説明

Cisco Cloudlockは、クラウドへの安全な移行を支援するクラウドネイティブのクラウドアクセスセキュリティブローカー（CASB）です。クラウドユーザー、データ、アプリを保護します。Cisco Cloudlockは、可視性とコンプライアンスチェックを提供し、データを誤用や流出から保護し、ランサムウェアなどのマルウェアに対する脅威から保護します。

質問: 205

組織は、ネットワーク上にマイクロセグメンテーションを実装しようとしており、ネットワーク内のアプリケーションの可視性を取得できるようにしたいと考えています。ソリューションは、コンプライアンスを維持および強制する必要があります。

これらの要件を満たすためにどの製品を使用する必要がありますか？

- A. Cisco Umbrella
- B. Cisco AMP
- C. Cisco Stealthwatch

D. Cisco Tetration

正解: ([正解を表示します](#))

説明

マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。

Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。

正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。

参照：

/solution-overview-c22-739268.pdf

質問: 206

エンジニアがルーターに安全に接続しようとしており、安全でないアルゴリズムが使用されないようにしたいと考えています。

ただし、接続は失敗しています。この目標を達成するためにどのような行動を取るべきですか？

- A. ip sshport22コマンドを使用してポートを設定します。
- B. ipsshserverコマンドを使用してSSHサーバーを有効にします。
- C. noiptelnetコマンドを使用してtelnetを無効にします。
- D. crypto keygeneratersaコマンドを使用してRSAキーを生成します。

正解: ([正解を表示します](#))

説明

<https://learningnetwork.cisco.com/s/question/0D53i00000KsrhK/rsa-key>

質問: 207

ハイブリッド電子メールソリューションを導入する場合、オンプレミス機器として残しておく必要がある2つのサービスはどれですか。 2つ選択してください)

- A. DDoS
- B. スパム対策
- C. ウイルス対策
- D. 暗号化
- E. DLP

正解: ([正解を表示します](#))

Cisco Hybrid Email Securityは、クラウドベースのEメールセキュリティの導入とアプライアンスベースのEメールセキュリティの導入（オンプレミス）を組み合わせ、組織に最大限の選択肢と制御を提供する独自のサービスです。クラウドベースのインフラストラクチャは通常、受信メールのクレンジングに使用されますが、オンプレミスアプライアンスはきめ細かい制御を提供し、データ損失防止（DLP）と暗号化テクノロジーで機密情報を保護します。

Cisco Hybrid Email Securityは、クラウドベースのEメールセキュリティの導入とアプライアンスベースのEメールセキュリティの導入（オンプレミス）を組み合わせ、組織に最大限の選択肢と制御を提供する独自のサービスです。クラウドベースのインフラストラクチャは通常、受信メールのクレンジングに使用されますが、オンプレミスアプライアンスはきめ細かい制御を提供し、データ損失防止（DLP）と暗号化テクノロジーで機密情報を保護します。

参照：

Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

Cisco Hybrid Email Securityは、クラウドベースのEメールセキュリティの導入とアプライアンスベースのEメールセキュリティの導入（オンプレミス）を組み合わせ、組織に最大限の選択肢と制御を提供する独自のサービスです。クラウドベースのインフラストラクチャは通常、受信メールのクレンジングに使用されますが、オンプレミスアプライアンスはきめ細かい制御を提供し、データ損失防止（DLP）と暗号化テクノロジーで機密情報を保護します。

Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

質問: 208

展示を参照してください。

```
> show crypto ipsec sa
interface: Outside
  Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
  209.165.200.225

    access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
    255.255.255.0 10.0.10.0 255.255.255.0
    local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
    current_peer: 209.165.202.129

    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
    209.165.202.129/500
    path mtu 1500, ipsec overhead 55(36), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: B6F5EA53
    current inbound spi : 84348DEF
```

トラフィックは、FirepowerThreatDefenseアプライアンスのIPsecサイト間VPNを通過していません。この問題の原因は何ですか？

A. アクセス制御ポリシーはでVPNトラフィックを許可していません。

- B. サイト間VPN事前共有キーが一致していません。
- C. サイト間VPNピアは異なる暗号化アルゴリズムを使用しています。
- D. FirepowerThreatDefenseアプライアンスで分割トンネルポリシーが定義されていません。
- 正解: ([正解を表示します](#))

質問: 209

組織はCiscoUmbrellを使用してURLブロッキングを実装しています

a。ユーザーはいくつかのサイトに行くことができます

しかし、エラーのために他のサイトにアクセスできません。エラーが発生するのはなぜですか？

- A. クライアントコンピュータにCisco UmbrellaRootCA証明書がインストールされていません。
- B. IP層の強制が構成されていません。
- C. クライアントコンピュータには、内部CAサーバーから展開されたSSL証明書がありません。
- D. インテリジェントプロキシとSSL復号化がポリシーで無効になっています

正解: ([正解を表示します](#))

説明説明その他の機能はSSL復号化機能に依存しており、CiscoUmbrellaルート証明書が必要です。SSL復号化機能を使用すると、次のことが向上します。カスタムURLブロック-HTTPS バージョンのURLをブロックするために必要です。... Umbrellaのブロックページおよびブロックページバイパス機能は、HTTPSサイトに接続するブラウザにSSL証明書を提示します。このSSL証明書は要求されたサイトと一致しますが、Cisco Umbrella認証局 (CA)によって署名されます。CAがブラウザによって信頼されていない場合、エラーページが表示されることがあります。一般的なエラーには、「このWebサイトによって提示されたセキュリティ証明書は信頼できる認証局によって発行されたものではありません」(InternetExplorer)、
「サイトのセキュリティ証明書は信頼されていません！」などがあります。(Google Chrome)または「この接続は信頼されていません」(Mozilla Firefox)。エラーページが予想されますが、表示されるメッセージは混乱を招く可能性があるため、表示されないようにすることをお勧めします。これらのエラーページを回避するには、Cisco Umbrellaルート証明書をブラウザまたはユーザーのブラウザにインストールします (ネットワーク管理者の場合)。参照：
<https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>説明その他の機能はSSL復号化機能に依存しており、CiscoUmbrellaルート証明書が必要です。SSL復号化機能を使用すると、次のことが向上します。ネットワーク管理者です。参照：
<https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>説明その他の機能はSSL復号化機能に依存しており、CiscoUmbrellaルート証明書が必要です。SSL復号化機能を使用すると、次のことが向上します。ネットワーク管理者です。参照：
<https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>説明その他の機能はSSL復号化機能に依存しており、CiscoUmbrellaルート証明書が必要です。SSL復号化機能を使用すると、次のことが向上します。
カスタムURLブロック-HTTPS バージョンのURLをブロックするために必要です。

..。

Umbrellaのブロックページおよびブロックページバイパス機能は、HTTPSサイトに接続するブラウザにSSL証明書を提示します。このSSL証明書は要求されたサイトと一致しますが、Cisco Umbrella認証局 (CA)によって署名されます。CAがブラウザによって信頼されていない場合、エラーページが表示されることがあります。

一般的なエラーには、「このWebサイトによって提示されたセキュリティ証明書は信頼できる認証局によって発行されたものではありません」

(InternetExplorer)、
「サイトのセキュリティ証明書は信頼されていません！」などがあります。(Google Chrome)または「この接続は信頼されていません」(MozillaFirefox)。エラーページが予想されますが、表示されるメッセージは混乱を招く可能性があるため、表示されないようにすることをお勧めします。

これらのエラーページを回避するには、Cisco Umbrellaルート証明書をブラウザまたはユーザーのブラウザにインストールします (ネットワーク管理者の場合)。

説明説明その他の機能はSSL復号化機能に依存しており、Cisco Umbrellaルート証明書が必要です。SSL復号化機能を使用すると、次のことが向上します。カスタムURLブロック-HTTPS バージョンのURLをブロックするために必要です。... Umbrellaのブロックページおよびブロックページバイパス機能は、HTTPSサイトに接続するブラウザにSSL証明書を提示します。このSSL証明書は要求されたサイトと一致しますが、Cisco Umbrella認証局 (CA)によって署名されます。CAがブラウザによって信頼されていない場合、エラーページが表示されることがあります。一般的なエラーには、「このWebサイトによって提示されたセキュリティ証明書は信頼できる認証局によって発行されたものではありません」(Internet Explorer)、"サイトのセキュリティ証明書は信頼されていません!"などがあります。(Google Chrome)または「この接続は信頼されていません」(Mozilla Firefox)。エラーページが予想されますが、表示されるメッセージは混乱を招く可能性があるため、表示されないようにすることをお勧めします。これらのエラーページを回避するには、Cisco Umbrellaルート証明書をブラウザまたはユーザーのブラウザにインストールします (ネットワーク管理者の場合)。参照：
<https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>

質問: 210

エンドポイントベースのセキュリティがソリューションとなるシナリオはどれですか？

- A. パスワードで保護されたアーカイブの検査
- B. デバイスのプロファイリングと承認
- C. 署名ベースのアプリケーション制御の実行
- D. 暗号化されたトラフィックの検査

正解: ([正解を表示します](#))

質問: 211

Cisco Application Visibility and Controlを使用して、ユーザがアプリケーションの使用状況とパフォーマンスの統計をエクスポートできるサービスはどれですか。

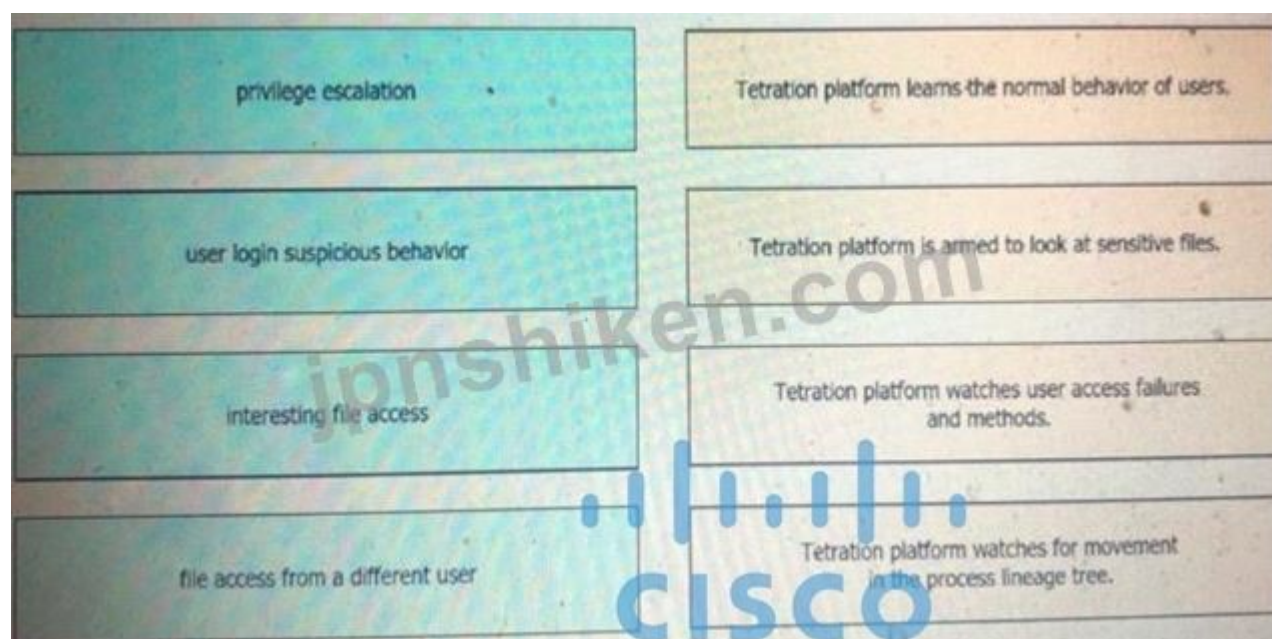
- A. 802.1X
- B. SNORT
- C. SNMP
- D. NetFlow

正解: ([正解を表示します](#))

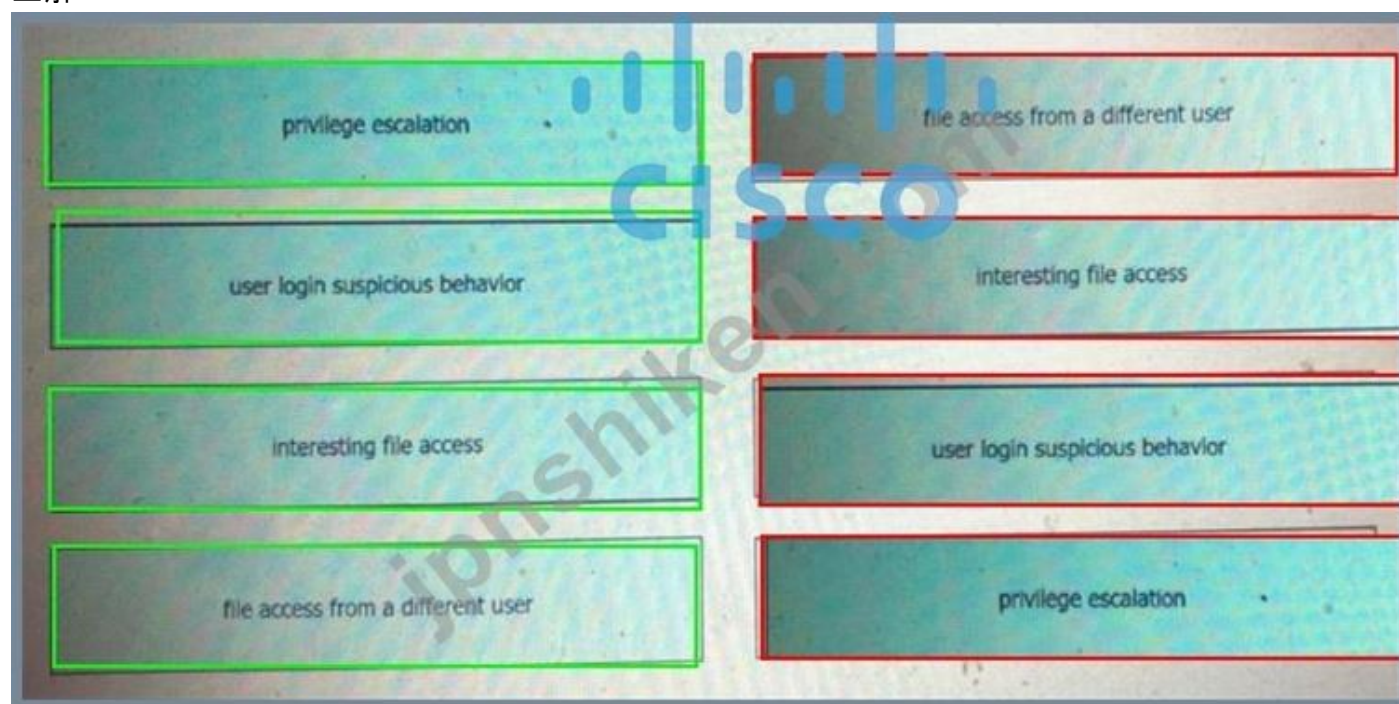
有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 212

Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。



正解:



質問: 213

展示を参照してください。



ドメイン名からの長さやサブドメインの数など、DNS要求の任意の機能を使用して、観測値を比較できる予想される動作のモデルを構築できることを考慮してください。これらの値はどのタイプの悪意のある攻撃に関連付けられていますか？

- A. ハートブリードSSLバグ
- B. スペクターワーム
- C. W32/AutoRunワーム
- D. 永遠の青い窓

正解: ([正解を表示します](#))

質問: 214

組織は、ネットワーク上にマイクロセグメンテーションを実装しようとしており、ネットワーク内のアプリケーションの可視性を取得できるようにしたいと考えています。ソリューションは、コンプライアンスを維持および強制する必要があります。これらの要件を満たすためにどの製品を使用する必要がありますか？

- A. Cisco Umbrella
- B. Cisco AMP
- C. Cisco Stealthwatch
- D. Cisco Tetration

正解: D ([コメントを發表する](#))

説明説明マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。正確なマイクロセグメンテーションポリシーを生成するには、Cisco Tetrationは、アプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベア

メタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。アプリケーションの動作が変化したときに、セグメンテーションポリシーが最新であることを確認します。参照 <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf> 説明マイクロセグメンテーションは、特定のアプリケーションを明示的に許可することにより、アプリケーションを保護します。トラフィックと、デフォルトでは、他のすべてのトラフィックを拒否します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。説明説明マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。正確なマイクロセグメンテーションポリシーを生成するには、Cisco Tetrationは、アプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。アプリケーションの動作が変化したときに、セグメンテーションポリシーが最新であることを確認します。参照 <https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf>

質問: 215

2つのDDoS攻撃カテゴリとは何ですか？ 2つ選択してください。）

- A. シーケンシャル
- B. プロトコル
- C. データベース
- D. ボリュームベース
- E. ガラ場ベース

正解: ([正解を表示します](#))

参照 :

<https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html>

質問: 216

管理者は、環境をより安全にするためにDHCPサーバーを構成しています。トラフィックをレート制限し、正当な要求がドロップされないようにする必要があります。これはどのように達成されますか？

- A. DHCPスヌーピングデータベースにエントリを追加します
- B. 必要なVLANのARP検査を有効にします
- C. DHCPスヌーピングビットを1に設定します
- D. DHCPサーバーの信頼できるインターフェースを設定します

正解: ([正解を表示します](#))

質問: 217

DMVPNテクノロジーとFlexVPNテクノロジーの共通点は何ですか？

- A. FlexVPNとDMVPNは、IS-ISルーティングプロトコルを使用してスポークと通信します
- B. FlexVPNとDMVPNは新しいキー管理プロトコルを使用します
- C. FlexVPNとDMVPNは同じハッシュアルゴリズムを使用します
- D. IOSルーターはDMVPNとFlexVPNに対して同じNHRPコードを実行します

正解: **D** ([コメントを发表する](#))

説明本質的に、FlexVPNはDMVPNと同じです。デバイス間の接続は引き続きポイントツーポイントGREトンネルであり、スポークツースポーク接続はNHRPリダイレクトメッセージで引き続き実現されます。IOSルータはDMVPNとFlexVPNの両方で同じNHRPコードを実行します。これは、両方がCisco独自のテクノロジーであることも意味します。。参照 <https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/> 本質的に、FlexVPNはDMVPNと同じです。デバイス間の接続は引き続きポイントツーポイントGREトンネルであり、スポークツースポーク接続はNHRPリダイレクトメッセージで引き続き実現されます。IOSルータはDMVPNとFlexVPNの両方で同じNHRPコードを実行します。これは、両方がCisco独自のテクノロジーであることも意味します。。

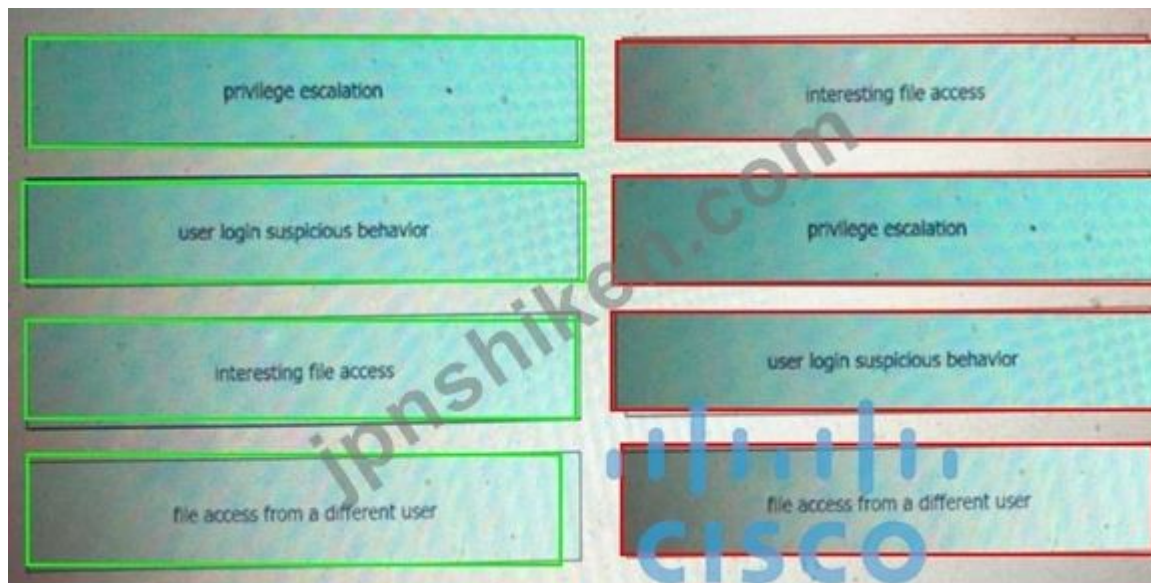
説明本質的に、FlexVPNはDMVPNと同じです。デバイス間の接続は引き続きポイントツーポイントGREトンネルであり、スポークツースポーク接続はNHRPリダイレクトメッセージで引き続き実現されます。IOSルータはDMVPNとFlexVPNの両方で同じNHRPコードを実行します。これは、両方がCisco独自のテクノロジーであることも意味します。。参照 <https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/>

質問: 218

Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。



正解:



質問: 219

システム管理者がWebトラフィックをWebセキュリティアプライアンスに透過的に送信する2つの方法はどれですか。(2つ選択してください。)

- A. ウェブブラウザの設定でプロキシIPアドレスを設定します
- B. 10.255.254.1バージョン3myv3内のsnmp-serverホスト
- C. プロキシ設定をプッシュするようにActiveDirectoryグループポリシーを構成する
- D. ネットワークインフラストラクチャでポリシーベースのルーティングを構成する
- E. プロキシ自動設定ファイルを参照する

正解: ([正解を表示します](#))

質問: 220

展示を参照してください。

Interface	MAC Address	Method	Domain	Status	Fg	Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth		0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth		0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth		0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth		0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth		0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth		0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth		0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth		0A02198200000
Gi8/14	c85b.7604.fald	dot1x	DATA	Auth		0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth		0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth		0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth		0A02198200000
Gi8/29	68bd.aba5.2844	dot1x	VOICE	Auth		0A02198200001
Gi7/4	54ee.750b.d966	dot1x	DATA	Auth		0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth		0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth		0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth		0A02198200000

この出力を生成し、どのポートがdot1xまたはmabで認証されているかを示すために使用されたコマンドはどれですか。

- A. 認証登録を表示する
 - B. dot1xallを表示
 - C. 認証方法を表示
 - D. 認証セッションを表示
- 正解: B (コメントを发表する)

質問: 221

CiscoFirepowerのセキュリティインテリジェンスポリシーを使用します。Firepowerブロックベースの2つの基準はどれですか。
(2つ選択してください。)

- A. プロトコルID
 - B. URL
 - C. IPアドレス
 - D. ポート番号
 - E. MACアドレス
- 正解: B,C (コメントを发表する)

説明

Security Intelligence Sources

- System-provided feeds

Cisco provides access to regularly updated intelligence feeds for domains, URLs and IP addresses.

質問: 222

展示を参照してください。

Interface	MAC Address	Method	Domain	Status	Eg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

この出力を生成し、どのポートがdot1xまたはmabで認証されているかを示すために使用されたコマンドはどれですか。

- A. 認証登録を表示する
- B. dot1xallを表示
- C. 認証方法を表示
- D. 認証セッションを表示

正解: [\(正解を表示します\)](#)

質問: 223

エンドポイントがIDグループから削除されたときに、エンドポイントセッションの再認証を強制するには、Cisco ISEで何を設定する必要がありますか。

- A. 姿勢評価
- B. CoA
- C. 外部IDソース
- D. SNMPプローブ

正解: B [\(コメントを发表する\)](#)

Cisco ISEでは、グローバルコンフィギュレーションで[ProfilerConfiguration]ページで[Changeof Authorization CoA)]を発行できます。これにより、プロファイリングサービスは、すでに認証されているエンドポイントをより詳細に制御できます。CoAタイプを構成するための設定の1つは、再認証」です。このオプションは、プロファイリング時に、すでに認証されているエンドポイントの再認証を強制するために使用されます。参照：

https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010101.htmlページ。すでに認証されています。

CoAタイプを構成するための設定の1つは、再認証」です。このオプションは、プロファイリング時に、すでに認証されているエンドポイントの再認証を強制するために使用されます。

参照：

Cisco ISEでは、グローバルコンフィギュレーションで[ProfilerConfiguration]ページで[Changeof Authorization CoA)]を発行できます。これにより、プロファイリングサービスは、すでに認証されているエンドポイントをより詳細に制御できます。CoAタイプを構成するための設定の1つは、再認証」です。このオプションは、プロファイリング時に、すでに認証されているエンドポイントの再認証を強制するために使用されます。参照：

https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010101.html

質問: 224

Cisco UmbrellaでWebポリシーが設定されている場合、マルウェア、コマンドアンドコントロール、フィッシング、およびその他の脅威をホストするときにドメインがブロックされるようにする機能を提供するものは何ですか。

- A. アプリケーション制御
- B. セキュリティカテゴリのブロック
- C. コンテンツカテゴリのブロック
- D. ファイル分析

正解: ([正解を表示します](#))

説明/参照 <https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories>

質問: 225

2つのルートキットタイプとは何ですか？ 2つ選択してください)

- A. レジストリ
- B. 仮想
- C. ブートローダー
- D. ユーザーモード
- E. バッファモード

正解: ([正解を表示します](#))

「ルートキット」という用語は元々Unixの世界に由来し、「ルート」という言葉は、Windowsの「管理者」と同様に、可能な限り最高レベルのアクセス権限を持つユーザーを表すために使用されます。「キット」という言葉は、マシンへのルートレベルのアクセスを許可するソフトウェアを指します。この2つを組み合わせると、「ルートキット」が得られます。これは、正当な意図または悪意のある意図を持った誰かに、コンピューターへの特権アクセスを提供するプログラムです。

ルートキットには、カーネルルートキット、ユーザーモードルートキット、ブートローダールートキット、メモリルートキットの4つの主要なタイプがあります。

質問: 226

Secure Internet Gatewayのマルウェアファイルスキャンを有効にするために必要な前提条件は何ですか？

- A. IP層の実施を有効にします。
- B. SSL復号化を有効にします。
- C. AdvancedMalwareProtectionライセンスをアクティブ化する
- D. インテリジェントプロキシを有効にします。

正解: C ([コメントを發表する](#))

有効的な**350-701**問題集はJPNTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTest.comは今最新**350-701**試験問題集を提供します。JPNTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 227

管理者は、既存の展開に新しいCiscoISEノードを追加しています。FQDNを入力するときにノードの追加が成功するようにするには、何をする必要がありますか？

- A. 新しいCiscoISEノードのDNSエントリをDNSサーバに追加します
- B. プライマリに登録する前に、新しいCiscoISEノードをセカンダリPANにします。
- C. CiscoISEノード間のファイアウォールでポート8905を開きます
- D. 新しいCiscoISEノードのIPアドレスを他のノードと同じネットワークに変更します。

正解: ([正解を表示します](#))

質問: 228

クラウドでのデータ侵害を防ぐために使用される2つのパラメーターはどれですか？ 2つ選択してください。)

- A. 暗号化
- B. DLPソリューション
- C. なりすまし防止プログラム
- D. 複雑なクラウドベースのWebプロキシ
- E. 強力なユーザー認証

正解: ([正解を表示します](#))

質問: 229

CiscoルータでNetflowエクスポートを設定するときに必要なパラメータはどれですか。

- A. DSCP値
- B. ソースインターフェース
- C. エクスポート名
- D. エクスポートの説明

正解: C ([コメントを發表する](#))

説明

NetFlowエクスポートを設定する例を以下に示します。

フローエクスポートエクスポート

宛先192.168.100.22

トランスポートUDP2055

質問: 230

多要素認証で最も一般的に使用される2つの認証要素は何ですか？ 2つ選択してください。)

```
HQ_Router(config)# username admin5 privilege 5
HQ_Router(config)#privilege interface level 5 shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5 description
```

- A. 知識要素
- B. 暗号化係数
- C. 時間係数
- D. 守秘義務

E. 生体認証係数

正解: ([正解を表示します](#))

質問: 231

組織のネットワークに接続するマシンに、組織のマルウェアの発生を防ぐために推奨されるウイルス対策の定義とパッチがあることを保証するシスコのプラットフォームはどれですか。

A. Cisco WiSM

B. Cisco ESA

C. Cisco ISE

D. Cisco Prime Infrastructure

正解: C ([コメントを發表する](#))

ポスチャポリシーは、1つ以上のIDグループとオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。[ワークセンター]>[ポスチャ]>[ポスチャ要素]>[条件]>[ファイル]でWindowsパッチをチェックするようにISEを設定できます。

この例では、事前定義されたファイルチェックを使用して、Windows10クライアントにWannaCryマルウェアを防ぐための重要なセキュリティパッチがインストールされていることを確認します。また、このパッチでクライアントを更新するようにISEを構成することもできます。

File Conditions List > pc_W10_64_KB4012606_Ms17-010_1507_W

File Condition

* Name **pc_W10_64_KB4012606_Ms1**

Description **Cisco Predefined Check: Micro**

* Operating System

Compliance Module **Any version**

* File Type ⓘ

* File Path

* Operator

* File Version **10.0.10240.17318**

質問: 232

組織は、接続が確立される前に悪意のある宛先をブロックすることにより、多層防御を改善しようとしています。ソリューションは、特定のアプリケーションがネットワーク内で使用されるのをブロックする必要があります。この目標を達成するには、どの製品を使用する必要がありますか？

- A. Cisco Firepower
- B. Cisco Umbrella
- C. ISE
- D. AMP

正解: ([正解を表示します](#))

説明

説明

Cisco Umbrellaは、接続が確立される前に、安全でない宛先を事前に分析してブロックすることにより、悪意のあるドメインへのアクセスからユーザーを保護します。したがって、攻撃者が送信した特定のリンクをクリックしたときに疑わしいドメインをブロックすることで、フィッシング攻撃から保護できます。

質問: 233

CoAがデバイスでサポートされるように、認証、許可、およびアカウントティングをグローバルに有効にするCiscoコマンドはどれですか。

- A. auth-type all
- B. aaa server radius dynamic-author
- C. ipデバイス追跡
- D. aaa new-model

正解: [\(正解を表示します\)](#)

質問: 234

クラウドセキュリティ評価コンポーネントを左側から右側の定義にドラッグアンドドロップします。

user entity behavior assessment	develop a cloud security strategy and roadmap aligned to business priorities
cloud data protection assessment	identify strengths and areas for improvement in the current security architecture during onboarding
cloud security strategy workshop	understand the security posture of the data or activity taking place in public cloud deployments
cloud security architecture assessment	detect potential anomalies in user behavior that suggest malicious behavior in a Software-as-a-Service application

正解:

user entity behavior assessment	cloud security strategy workshop
cloud data protection assessment	cloud data protection assessment
cloud security strategy workshop	cloud security architecture assessment
cloud security architecture assessment	user entity behavior assessment

質問: 235

```

import requests

client_id = 'a1b2c3d4e5'

api_key = 'a1b2c3d4-e5f6-g7h8'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)

```

展示を参照してください。Ciscoセキュリティアプライアンスに接続すると、APIは何をしますか？

- A. AMPが認識しているコンピューターに関するネットワークインターフェイス情報を収集します
- B. ネットワーク内のコンピューターからプロセスとPID情報を取得します
- C. エンドポイントのAMPからネットワークテレメトリ情報を収集します
- D. AMPを管理するためのSNMPプルメカニズムを作成します

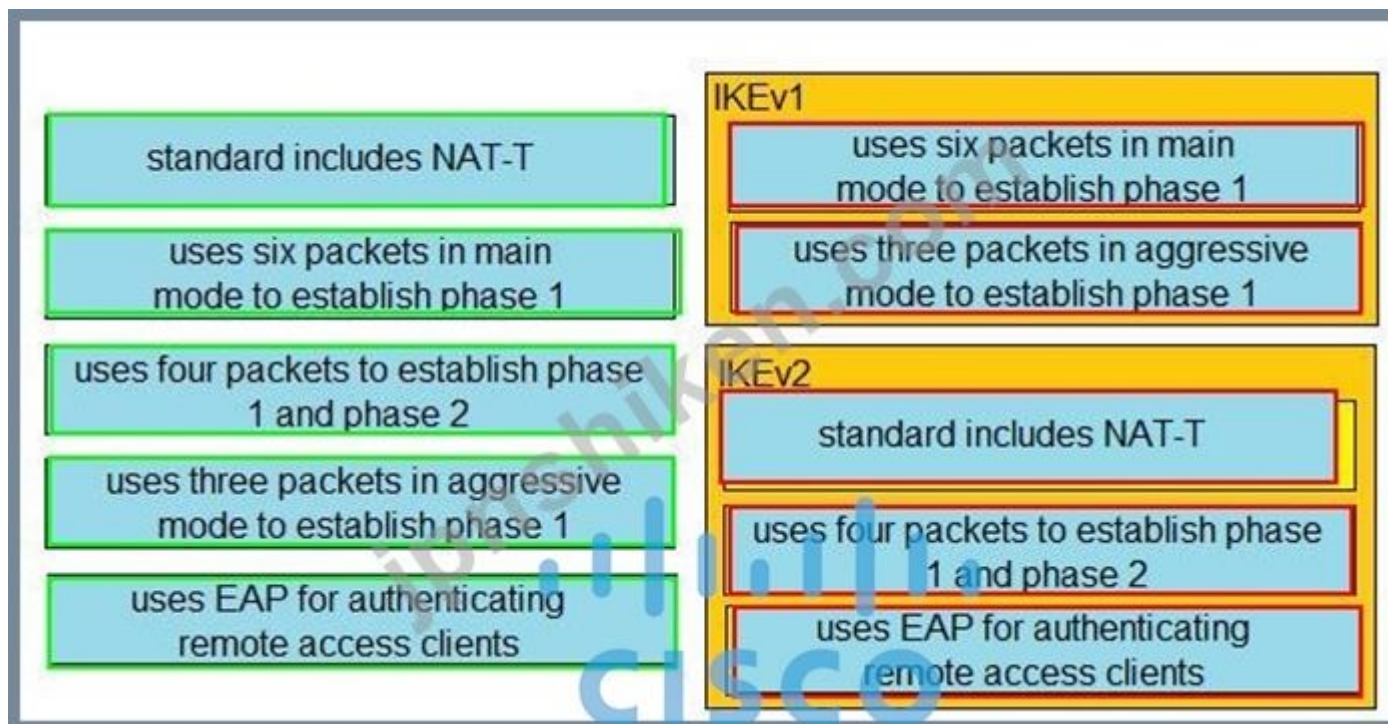
正解: [\(正解を表示します\)](#)

質問: 236

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

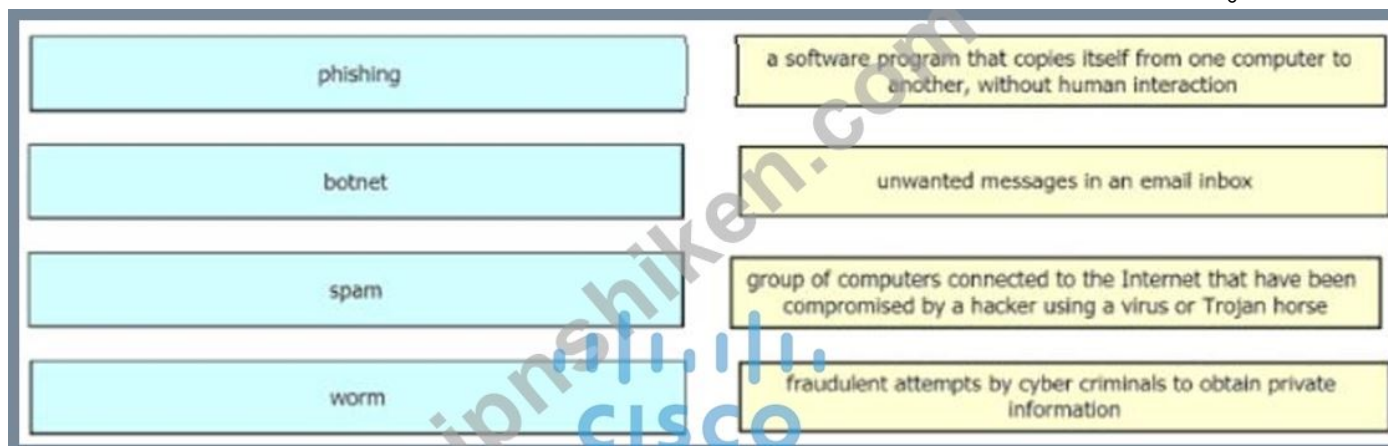
standard includes NAT-T	IKEv1
uses six packets in main mode to establish phase 1	
uses four packets to establish phase 1 and phase 2	IKEv2
uses three packets in aggressive mode to establish phase 1	
uses EAP for authenticating remote access clients	

正解:



質問: 237

一般的なセキュリティの脅威を左側から右側の定義にドラッグアンドドロップします。



正解:



質問: 238

CiscoASDMよりもCiscoFMCを使用する利点は何ですか。

- A. Cisco FMCはJavaを使用し、CiscoASDMはHTML5を使用します。
- B. Cisco FMCは集中管理を提供しますが、CiscoASDMは提供しません。
- C. Cisco FMCはデバイスへの設定のプッシュをサポートしていますが、CiscoASDMはサポートしていません。
- D. Cisco FMCはすべてのファイアウォール製品をサポートしますが、CiscoASDMはCiscoASAデバイスのみをサポートします

正解: ([正解を表示します](#))

Cisco FTDデバイス、Cisco Firepowerデバイス、およびCisco ASA FirePOWERモジュールは、以前はFireSIGHTManagementCenterと呼ばれていたFirepowerManagementCenter (FMC)で管理できます-回答Dは正しくありませんCisco FTDデバイス、Cisco Firepowerデバイス、およびCisco ASA FirePOWERモジュールは、以前はFireSIGHTManagementCenterと呼ばれていたFirepowerManagementCenter (FMC)で管理できます-回答Dは正しくありません参照：

注 ASA FirePOWERモジュールは、個別にアップグレードされたASAオペレーティングシステムで実行されます

FMCを使用してASAファイアウォール機能を管理することはできません。」

Cisco Secure Firewall Threat Defense Manager (Firepower Management Center)は、一元化され、統合され、合理化された管理を提供することにより、シスコのネットワークセキュリティソリューションの有効性を高めます。

Cisco FTDデバイス、Cisco Firepowerデバイス、およびCisco ASA FirePOWERモジュールは、以前はFireSIGHTManagementCenterと呼ばれていたFirepowerManagementCenter (FMC)で管理できます-回答Dは正しくありません注 ASAFirePOWERモジュールは個別に実行されますアップグレードされたASAオペレーティングシステム

FMCを使用してASAファイアウォール機能を管理することはできません。」

Cisco Secure Firewall Threat Defense Manager (Firepower Management Center)は、一元化され、統合され、合理化された管理を提供することにより、シスコのネットワークセキュリティソリューションの有効性を高めます。

注 ASA FirePOWERモジュールは、個別にアップグレードされたASAオペレーティングシステムで実行されます

FMCを使用してASAファイアウォール機能を管理することはできません。」

Cisco Secure Firewall Threat Defense Manager (Firepower Management Center)は、一元化され、統合され、合理化された管理を提供することにより、シスコのネットワークセキュリティソリューションの有効性を高めます。

質問: 239

エンジニアは、ホスト上の悪意のあるアクティビティを検出するために動作分析を必要とし、クラウドプロバイダーのメカニズムを使用してテレメトリをセキュリティデバイスに送信するように組織のパブリッククラウドを構成しています。この目標を達成するために、エンジニアはどのメカニズムを構成する必要がありますか？

- A. ミラーポート
- B. NetFlow
- C. フロー
- D. VPCフローログ

正解: ([正解を表示します](#))

<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/q-and-a-c67-737402.html>

質問: 240

エンジニアは、CiscoASAを通過するトラフィックに関するNetFlowレコードを生成したいと考えています。どのCiscoASAコマンドを使用する必要がありますか。

- A. フローエクスポーター<名前>
- B. ip flow-export destination 1.1.1.1 2055
- C. 1.1.1.12055内のフローエクスポート先
- D. ip flow monitor <name> input

正解: ([正解を表示します](#))

質問: 241

ネットワークエンジニアは、ネットワークに新しい医療機器を追加する任務を負っています。Cisco ISEがNACサーバとして使用されており、新しいデバイスには使用可能なサブリカントがありません。このデバイスをネットワークに安全に接続するには、何をする必要がありますか？

- A. プロファイリングでMABを使用する
- B. 姿勢評価でMABを使用します。
- C. 姿勢評価で802.1Xを使用します。
- D. プロファイリングで802.1Xを使用します。

正解: ([正解を表示します](#))

説明説明新しいデバイスにはサブリカントがないため、802.1Xを使用できません。MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意の識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づいて、ユーザーに差別化されたネットワークアクセスを提供することです。例えば、従業員は、会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。参照 <https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456>説明新しいデバイスにはサブリカントがないため、802.1Xを使用できません。

MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意の識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。

分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づ

いて、ユーザーに差別化されたネットワークアクセスを提供することです。たとえば、従業員は会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。説明説明新しいデバイスにはサブリカントがないため、802.1Xを使用できません。MAC認証バイパス (MAB)は、802.1xをサポートしないデバイスのフォールバックオプションです。事実上、何らかの形または形式で展開に使用されます。MABは、オーセンティケーターに接続デバイスのMACアドレスを取得させ、それをユーザー名とパスワードとして認証サーバーに送信させることで機能します。認証サーバーはポリシーをチェックし、802.1xの場合と同じようにAccess-AcceptまたはAccess-Rejectを送り返します。Cisco ISEプロファイリングサービスは、ネットワークに接続されているエンドポイントの動的な検出と分類を提供します。ISEは、MACアドレスを一意的識別子として使用して、各ネットワークエンドポイントのさまざまな属性を収集し、内部エンドポイントデータベースを構築します。分類プロセスでは、収集された属性を事前に作成された条件またはユーザー定義の条件と照合します。これらの条件は、プロファイルの広範なライブラリに関連付けられます。これらのプロファイルには、モバイルクライアント (iPad、Androidタブレット、Chromebookなど)、デスクトップオペレーティングシステム (Windows、Mac OS X、Linuxなど)、および多数の非ユーザーを含む、さまざまな種類のデバイスが含まれます。プリンター、電話、カメラ、ゲームコンソールなどのシステム。分類されると、エンドポイントはネットワークに対して許可され、プロファイルに基づいてアクセスが許可されます。たとえば、IP電話プロファイルに一致するエンドポイントは、認証方法としてMAC認証バイパス (MAB)を使用して音声VLANに配置できます。もう1つの例は、使用するデバイスに基づいて、ユーザーに差別化されたネットワークアクセスを提供することです。例えば、従業員は、会社のワークステーションからネットワークにアクセスするときにフルアクセスを取得できますが、個人のiPhoneからネットワークにアクセスするときは制限付きのネットワークアクセスが許可されます。参照 <https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456>

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **242**

展示を参照してください。



管理者が新しいCiscoFTDデバイスをネットワークに追加していて、CiscoFMCで管理したいと考えています。CiscoFTDはNATデバイスの背後にありません。Cisco FTDでこれを有効にするには、どのコマンドが必要ですか。

- A. マネージャーを構成してDONTRESOLVE登録キーを追加>
- B. configure manager add <FMC IP address> <registration key> 16
- C. configure manager addDONTRESOLVE<登録キー>FTD123

D. configure manager add <FMC IP address> <registration key>

正解: ([正解を表示します](#))

説明説明FMCにFTDを管理させるには、最初にFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド configuremanageradd 1.1.1.2 the_registration_key_you_want (1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。参照 <https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/>説明FMCにFTDを管理させるには、まずFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンドconfiguremanageradd 1.1.1.2 the_registration_key_you_want (1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。

説明説明FMCにFTDを管理させるには、最初にFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド configuremanageradd 1.1.1.2 the_registration_key_you_want (1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。参照 <https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/>

質問: 243

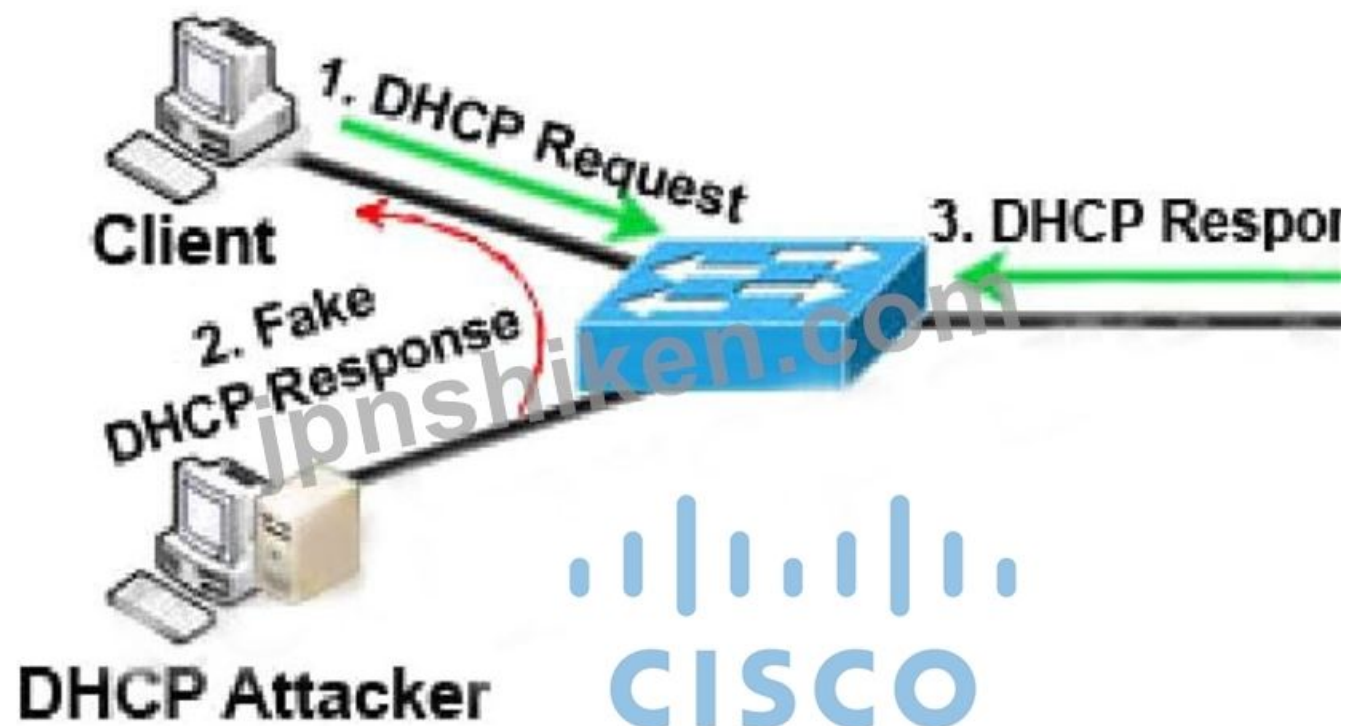
管理者は、環境をより安全にするためにDHCPサーバーを構成しています。トラフィックをレート制限し、正当な要求がドロップされないようにする必要があります。これはどのように達成されますか？

- A. DHCPサーバーの信頼できるインターフェースを設定します
- B. DHCPスヌーピングビットを1に設定します
- C. DHCPスヌーピングデータベースにエントリを追加します
- D. 必要なVLANのARP検査を有効にします

正解: ([正解を表示します](#))

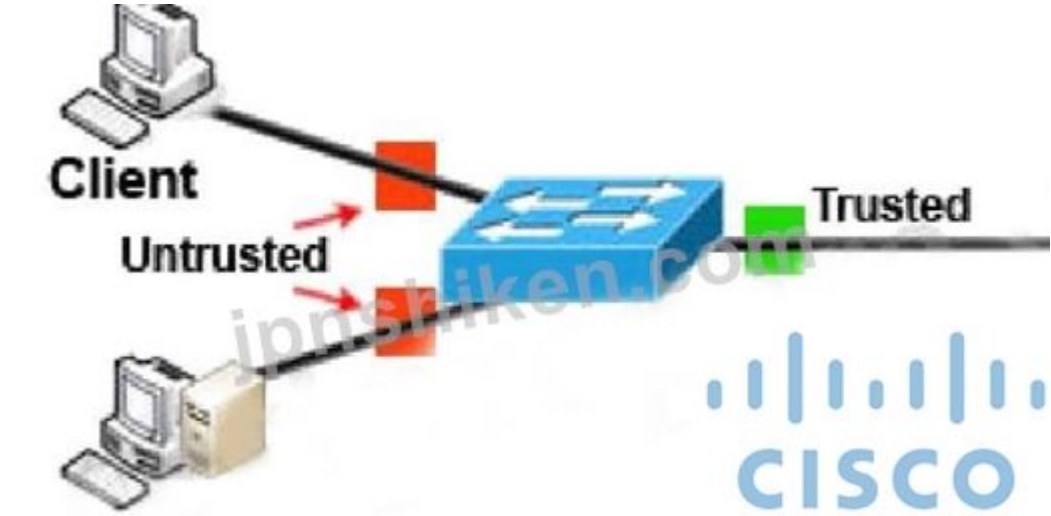
説明

DHCPスヌーピングを理解するには、最初にDHCPスプーフィング攻撃について学ぶ必要があります。



DHCPスプーフィングは、攻撃者がクライアントからのDHCP要求をリッスンし、許可されたDHCP応答がクライアントに到達する前に、偽のDHCP応答で応答するという攻撃の一種です。偽のDHCP応答は、多くの場合、クライアントのデフォルトゲートウェイとしてIPアドレスを提供します-クライアントから送信されるすべてのトラフィックは攻撃者のコンピュータを通過し、攻撃者は「中間者」になります。

攻撃者は、偽のDHCP応答が最初に到着することを確認するいくつかの方法があります。実際、攻撃者がDHCPサーバーよりも「近い」場合、攻撃者は何もする必要はありません。または、DHCPサーバーをDoSして、DHCP応答を送信できないようにすることもできます。DHCPスヌーピングは、DHCPスプーフィング攻撃を防ぐことができます。DHCPスヌーピングは、DHCP要求に応答できるスイッチポートを決定するCiscoCatalystの機能です。ポートは、信頼できるものと信頼できないものとして識別されます。



DHCP Attacker

許可されたDHCPサーバーに接続するポートのみが信頼され、すべての種類のDHCPメッセージの送信が許可されます。スイッチ上の他のすべてのポートは信頼されておらず、DHCP要求のみを送信できます。信頼できないポートでDHCP応答が見られる場合、ポートはシャットダウンされます。

質問: 244

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

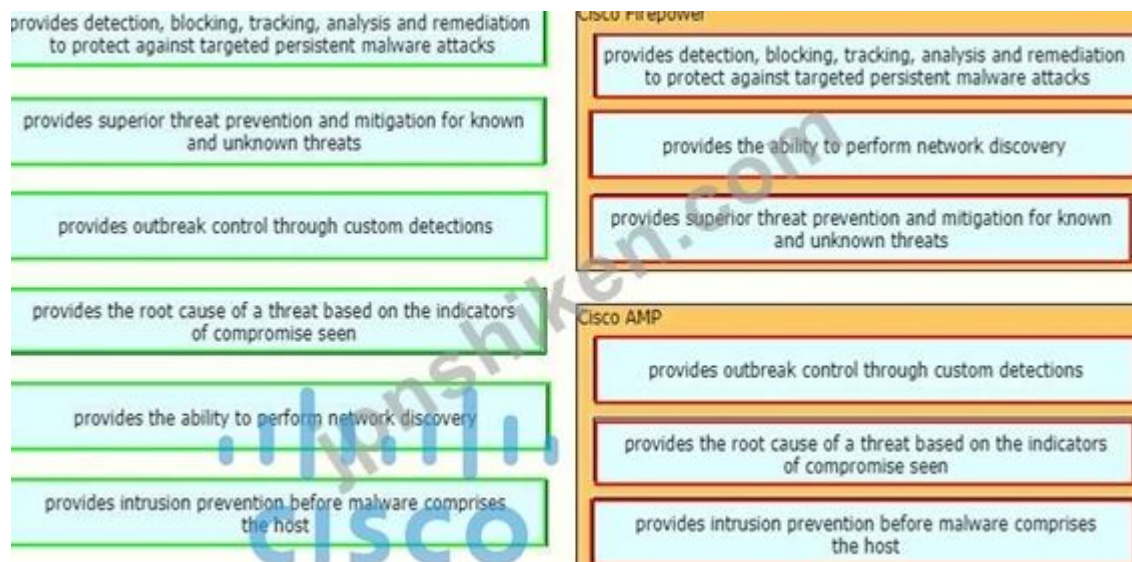
provides the ability to perform network discovery

provides intrusion prevention before malware compromises the host

Cisco Firepower

Cisco AMP

正解:



質問: 245

```
snmp-server group SNMP v3 auth access 15
```

展示を参照してください。この構成では、15という数字は何を表していますか？

- A. ルーターにアクセスできるSNMPデバイスを識別するアクセスリスト
- B. このルーターに対する許可されたユーザーの特権レベル
- C. SNMPv3認証の試行間の秒単位の間隔
- D. SNMPv3ユーザーがロックアウトされるまでに失敗した可能性のある試行の数

正解: [\(正解を表示します\)](#)

質問: 246

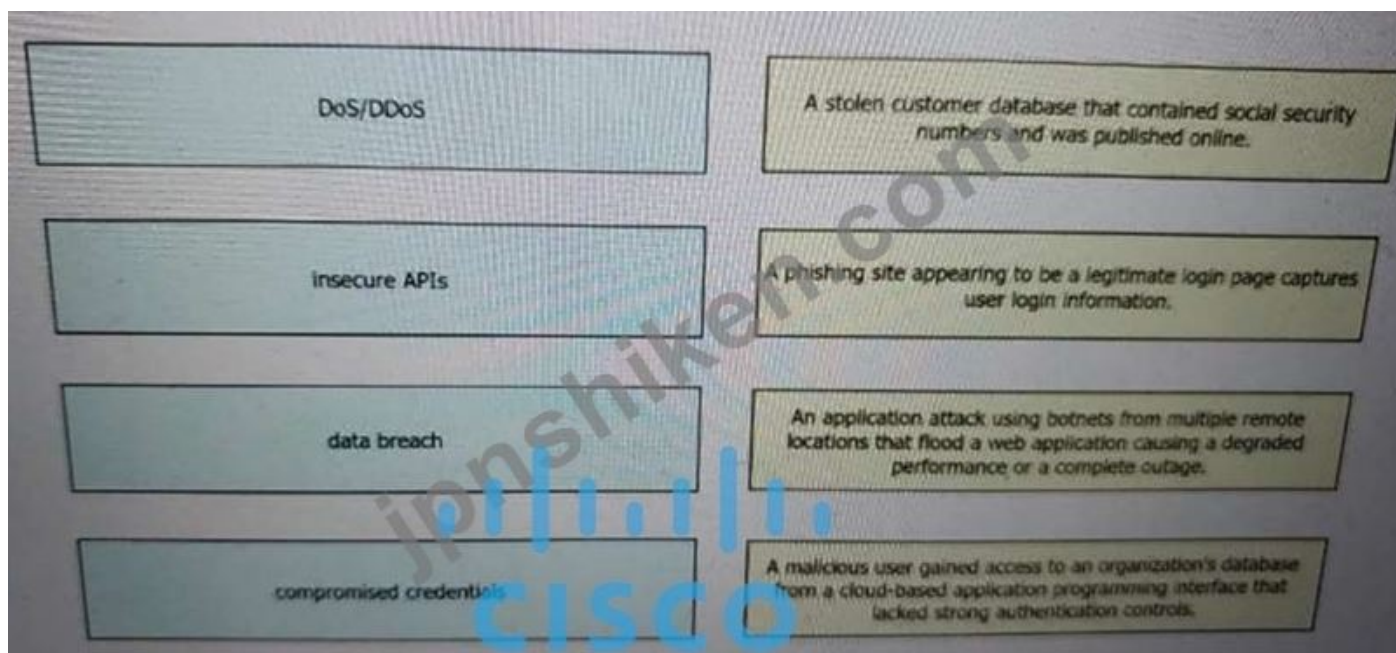
認証後にセッションのAAA属性を変更するメカニズムを提供するRADIUS機能はどれですか。

- A. 認証
- B. CoA
- C. 承認
- D. 会計

正解: B ([コメントを发表する](#))

質問: 247

脅威を左側から右側の脅威の例にドラッグアンドドロップします



正解:



質問: 248

CoAが発行されるのはどの2つの状況ですか？ 2つ選択してください。）

- A. 新しい認証ルールがポリシーサービスノードのポリシーに追加されました。
- B. IdentityServiceEngineサーバーでエンドポイントが削除されました。
- C. 新しいIDソースシーケンスが作成され、認証ポリシーで参照されます。
- D. エンドポイントが初めてプロファイルされます。
- E. 新しいIdentityServiceEngineサーバーが管理ペルソナとともに展開に追加されます。

正解: B,D (コメントを发表する)

説明/リファレンス https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

質問: 249

組織は、クラウド内のユーザー、データ、およびアプリケーションを保護したいと考えています。ソリューションはAPIベースであり、クラウドネイティブCASBとして動作する必要があります。この実装にはどのソリューションを使用する必要がありますか？

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco Cloud Email Security
- D. CiscoFirepower次世代ファイアウォール

正解: ([正解を表示します](#))

質問: 250

エンジニアは、ルーターの構成が侵害された場合に資格情報が表示されないようにするために、ルーターでデバイス強化を構成しています。どのコマンドを使用する必要がありますか？

- A. サービスパスワードの回復
- B. ユーザー名<ユーザー名>パスワード<パスワード>
- C. サービスパスワード暗号化
- D. ユーザー名<ユーザー名>特権15パスワード<パスワード>

正解: ([正解を表示します](#))

質問: 251

透過モードで実行されているCiscoWSAと明示モードで実行されているCiscoWSAの2つの違いは何ですか。 2つ選択してください)

- A. Cisco WSAが透過モードで実行されている場合、HTTP要求の宛先としてWSA自身のIPアドレスを使用します。
- B. Cisco WSAは、明示モードで実行されている場合にのみ、独自のIPアドレスで応答します。
- C. Cisco WSAは、透過モードで実行されている場合にのみWebブラウザで設定されます。
- D. Cisco WSAは、透過モードで実行されている場合にのみ、レイヤ3デバイスを使用してトラフィックをリダイレクトします。
- E. Cisco WSAは、透過モードで実行されている場合にのみ、独自のIPアドレスで応答します。

正解: D,E ([コメントを发表する](#))

説明

Cisco Webセキュリティアプライアンス (WSA)には、Webプロキシ、脅威分析エンジン、ウイルス対策エンジン、ポリシー管理、および単一の物理アプライアンスまたは仮想アプライアンスでのレポートが含まれています。Cisco WSAの主な用途は、悪意のあるWebサイトにアクセスしたりマルウェアに感染したりすることからユーザーを保護することです。

CiscoWSAは次の2つの異なるモードで導入できます。

-明示的な転送モード

-透過モード

明示的転送モードでは、クライアントはプロキシを明示的に使用するよう構成され、その後、すべてのWebトラフィックをプロキシに送信します。クライアントはプロキシが存在することを認識しており、すべてのトラフィックを明示的転送モードでプロキシに送信するため、クライアントはURLを要求する前にドメインのDNSルックアップを実行しません。Cisco WSAは、DNS解決も担当します。

Cisco WSAを明示モードで設定する場合、クライアント要求をCiscoWSAにリダイレクトするために他のネットワークインフラストラクチャデバイスを設定する必要はありません。ただし、CiscoWSAにトラフィックを送信するように各クライアントを設定する必要があります。->したがって、明示モードでは、WSAはクライアントとWebサーバー間のトラフィックのみをチェックします。WSAは独自のIPアドレスを使用して要求しません-回答Bは正しくありません。Cisco WSAが透過モードの場合、クライアントはプロキシが展開されていることを認識しません。ネットワークインフラストラクチャデバイスは、トラフィックをCiscoWSAに転送するように設定されています。透過モードの展開では、ネットワークインフラストラクチャデバイ

スはWebトラフィックをプロキシにリダイレクトします。Webトラフィックのリダイレクトは、ポリシーベースルーティング (PBR) (多くのルータで使用可能)を使用して、またはCisco ASAでCiscoのWebキャッシュ通信プロトコル (WCCP)を使用して実行できます。Ciscoルーターまたはスイッチ。Cisco Systemsによって開発されたWebCacheCommunication Protocol (WCCP)は、1つまたは複数のスイッチと1つまたは複数のWebキャッシュ間の相互作用を指定します。相互作用の目的は、ルーターのグループを流れるトラフィックの透過的なリダイレクトを確立して維持することです。参照：<https://www.cisco.com/c/en/us/tech/content-networking/web-cache-communications-protocol-wccp/index.html>→したがって、リダイレクトは実行できるため、回答Dは正しいです。レイヤ3デバイスのみ。透過モードでは、クライアントはトラフィックがプロキシ (Cisco WSA)に送信されていることに気づかず、その結果、クライアントはDNSを使用してURLのドメイン名を解決し、Webサーバ宛てのWeb要求を送信します (プロキシ)。Cisco WSAをトランスペアレントモードで設定する場合、クライアント要求をCisco WSAにリダイレクトするインフラストラクチャデバイス。ただし、Cisco WSAにトラフィックを送信するように各クライアントを設定する必要があります。

→したがって、明示モードでは、WSAはクライアントとWebサーバ間のトラフィックのみをチェックします。WSAは独自のIPアドレスを使用して要求しません-回答Bは正しくありません。

Cisco WSAが透過モードの場合、クライアントはプロキシが展開されていることを認識しません。ネットワークインフラストラクチャデバイスは、トラフィックをCisco WSAに転送するように設定されています。透過モードの展開では、ネットワークインフラストラクチャデバイスはWebトラフィックをプロキシにリダイレクトします。Webトラフィックのリダイレクトは、ポリシーベースルーティング (PBR) (多くのルータで使用可能)を使用するか、Cisco ASA、Ciscoルータ、またはスイッチでCiscoのWebキャッシュ通信プロトコル (WCCP)を使用して実行できます。

Cisco Systemsによって開発されたWebCacheCommunication Protocol (WCCP)は、1つまたは複数のスイッチと1つまたは複数のWebキャッシュ間の相互作用を指定します。相互作用の目的は、ルーターのグループを流れるトラフィックの透過的なリダイレクトを確立して維持することです。

参照：

→したがって、リダイレクトはレイヤ3デバイスでのみ実行できるため、回答Dは正しいです。

Cisco WSAを明示モードで設定する場合、クライアント要求をCisco WSAにリダイレクトするために他のネットワークインフラストラクチャデバイスを設定する必要はありません。ただし、Cisco WSAにトラフィックを送信するように各クライアントを設定する必要があります。→したがって、明示モードでは、WSAはクライアントとWebサーバ間のトラフィックのみをチェックします。WSAは独自のIPアドレスを使用して要求しません-回答Bは正しくありません。Cisco WSAが透過モードの場合、クライアントはプロキシが展開されていることを認識しません。ネットワークインフラストラクチャデバイスは、トラフィックをCisco WSAに転送するように設定されています。透過モードの展開では、ネットワークインフラストラクチャデバイスはWebトラフィックをプロキシにリダイレクトします。Webトラフィックのリダイレクトは、ポリシーベースルーティング (PBR) (多くのルータで使用可能)を使用して、またはCisco ASAでCiscoのWebキャッシュ通信プロトコル (WCCP)を使用して実行できます。Ciscoルーターまたはスイッチ。Cisco Systemsによって開発されたWebCacheCommunication Protocol (WCCP)は、1つまたは複数のスイッチと1つまたは複数のWebキャッシュ間の相互作用を指定します。相互作用の目的は、ルーターのグループを流れるトラフィックの透過的なリダイレクトを確立して維持することです。参照：<https://www.cisco.com/c/en/us/tech/content-networking/web-cache-communications-protocol-wccp/index.html>→したがって、リダイレクトは実行できるため、回答Dは正しいです。レイヤ3デバイスのみ。透過モードでは、クライアントはトラフィックがプロキシ (Cisco WSA)に送信されていることに気づかず、その結果、クライアントはDNSを使用してURLのドメイン名を解決し、Webサーバ宛てのWeb要求を送信します (プロキシ)。Cisco WSAをトランスペアレントモードで設定する場合、透過モードのWSA

→したがって、透過モードでは、WSAは独自のIPアドレスを使用してWebサーバに新しい接続を開始します (上記の手順4)→回答Eは正しいです。

どちらのモードでもWebブラウザでWSAを設定できないため、回答Cは確かに正しくありません。

回答Aは正しいようですが、そうではありません。この回答は、「Cisco WSAがトランスペアレントモードで実行されている場合、WSA自身のIPアドレスをHTTP要求の送信元 (宛先ではない)として使用する」と述べている場合に正解です。

質問: 252

展示を参照してください。

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                  = AUTHENTICATOR
PortControl          = FORCE_AUTHORIZED
ControlDirection    = Both
HostMode             = SINGLE_HOST
QuietPeriod         = 60
ServerTimeout        = 0
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30
```

この出力を表示するために使用されたコマンドはどれですか？

- A. dot1xを表示
- B. show dot1x interface gi1 / 0/12
- C. dot1xallを表示
- D. dot1xのすべての概要を表示

正解: C ([コメントを发表する](#))

質問: 253

Flexible NetFlowレコードの2つの利点は何ですか？ 2つ選択してください)

- A. ユーザーがフロー情報を構成してカスタマイズされたトラフィック識別を実行できるようにします
- B. トラフィックをドロップすることで攻撃を防止します
- C. アカウンティングと請求の機能強化を提供します
- D. 複数の会計技術を1つの会計メカニズムに統合します
- E. レイヤー2から4までの幅広いIPパケット情報の監視を提供します

正解: ([正解を表示します](#))

NetFlowは通常、次のようないくつかの主要な顧客アプリケーションに使用されます。...請求とアカウンティング。NetFlowデータは、非常に柔軟で詳細なリソース使用率アカウンティングのために、きめ細かいメータリング（たとえば、フローデータにはIPアドレス、パケット数とバイト数、タイムスタンプ、Type of Service (ToS)、アプリケーションポートなどの詳細が含まれます）を提供します。サービスプロバイダーは、時刻、帯域幅の使用量、アプリケーションの使用量、サービス品質などに基づいて請求に情報を使用する場合があります。企業のお客様は、この情報を部門のチャージバックまたはリソース使用率のコスト配分に使用できます。参照 <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnffnetflow.html>事前定義されている場合柔軟なNetFlowレコードは、トラフィック要件には適していません。Flexible NetFlowのcollectおよびmatchコマンドを使用して、ユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。参照 https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413_d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。これらのレイヤー。

...

請求と会計。NetFlowデータは、非常に柔軟で詳細なリソース使用率アカウンティングのために、きめ細かいメータリング（たとえば、フローデータにはIPアドレス、パケット数とバイト数、タイムスタンプ、サービスの種類（ToS）、アプリケーションポートなどの詳細が含まれます）を提供します。サービスプロバイダーは、時刻、帯域幅の使用量、アプリケーションの使用量、サービス品質などに基づいて請求に情報を使用する場合があります。企業のお客様は、この情報を部門のチャージバックまたはリソース使用率のコスト配分に使用できます。

参照：

事前定義されたFlexibleNetFlowレコードがトラフィック要件に適していない場合は、Flexible NetFlowの収集および一致コマンドを使用してユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。Flexible NetFlowは通常、これらを超えて、次のようないくつかの主要な顧客アプリケーションに使用されます。NetFlowデータは、非常に柔軟で詳細なリソース使用率アカウンティングのために、きめ細かいメータリング（たとえば、フローデータにはIPアドレス、パケット数とバイト数、タイムスタンプ、Type of Service（ToS）、アプリケーションポートなどの詳細が含まれます）を提供します。サービスプロバイダーは、時刻、帯域幅の使用量、アプリケーションの使用量、サービス品質などに基づいて請求に情報を使用する場合があります。企業のお客様は、この情報を部門のチャージバックまたはリソース使用率のコスト配分に使用できます。参照 <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnffnetflow.html>事前定義されている場合Flexible NetFlowレコードは、トラフィック要件には適していません。FlexibleNetFlowのcollectおよびmatchコマンドを使用して、ユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。参照：

<https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/>

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。これらのレイヤー。com / c / en / us / td / docs / ios-xml / ios / fnetflow / configuration / 15-mt / fnf-15-mt-book/fnffnetflow.html事前定義されたFlexibleNetFlowレコードがトラフィック要件に適していない場合、Flexible NetFlowの収集および照合コマンドを使用して、ユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。参照 <https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/>

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。これらのレイヤー。com / c / en / us / td / docs / ios-xml / ios / fnetflow / configuration / 15-mt / fnf-15-mt-book/fnffnetflow.html事前定義されたFlexibleNetFlowレコードがトラフィック要件に適していない場合、Flexible NetFlowの収集および照合コマンドを使用して、ユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。参照 <https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/>

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。これらのレイヤー。Flexible NetFlowのcollectおよびmatchコマンドを使用して、ユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。参照 <https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/>

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。これらのレイヤー。Flexible NetFlowのcollectおよびmatchコマンドを使用して、ユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。参照 <https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/>

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来のNetFlowでは、レイヤー2から4までの監視が可能です。これらのレイヤー。

質問: 254

PKIでのCAの目的は何ですか？

- A. デジタル証明書を発行および取り消す
- B. デジタル証明書の信頼性を検証する
- C. デジタル証明書の秘密鍵を作成するには
- D. 指定されたサブジェクトによる公開鍵の所有権を証明するため

正解: A ([コメントを发表する](#))

信頼できるCAは、信頼できるデジタル証明書を発行できる唯一のエンティティです。PKIはこれらの証明書の暗号化側の多くを管理しますが、認証はどのエンティティがどのキーを所有しているかを理解するために不可欠であるため、これは非常に重要です。信頼できるCAがなければ、誰でも自分のキーを発行でき、認証はウィンドウの外に出て、混乱が生じます。参照 <https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/> 信頼できるCAは、信頼できるデジタル証明書を発行できる唯一のエンティティです。PKIはこれらの証明書の暗号化側の多くを管理しますが、認証はどのエンティティがどのキーを所有しているかを理解するために不可欠であるため、これは非常に重要です。信頼できるCAがなければ、誰でも自分のキーを発行でき、認証はウィンドウの外に出て、混乱が生じます。参照 <https://>

質問: 255

ネットワークエンジニアは、VMware vMotionを使用して、CiscoWSA仮想アプライアンスをある物理ホストから別の物理ホストに移行する必要があります。両方の物理ホストの要件は何ですか？

- A. ホストは仮想アプライアンスとは異なるデータストアを使用する必要があります。
- B. ホストは同じ定義済みネットワークにアクセスできる必要があります。
- C. ホストは異なるバージョンのCiscoAsyncOSを実行する必要があります。
- D. ホストはCiscoAsyncOS10.0以降を実行している必要があります。

正解: D ([コメントを发表する](#))

質問: 256

Dos攻撃が含まれるカテゴリはどれですか？

- A. フィッシング攻撃
- B. 洪水攻撃
- C. トロイの木馬攻撃
- D. ウイルス攻撃

正解: B ([コメントを发表する](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 257

シスコ内のどのグループが週刊ニュースレターを作成および発行して、サイバーセキュリティの専門家が進行中の最も蔓延している脅威を認識し続けるのを支援していますか？

- A. PSIRT
- B. タロス
- C. CSIRT
- D. DEVNET

正解: **B** ([コメントを发表する](#))

Talos Threat Sourceは、Cisco Talosからの定期的なインテリジェンスアップデートであり、毎週最大の脅威やその他のセキュリティニュースを強調しています。

Talos Threat Sourceは、Cisco Talosからの定期的なインテリジェンスアップデートであり、毎週最大の脅威やその他のセキュリティニュースを強調しています。

Talos Threat Sourceは、Cisco Talosからの定期的なインテリジェンスアップデートであり、毎週最大の脅威やその他のセキュリティニュースを強調しています。

質問: **258**

AWSパブリッククラウド内にCiscoASAvをデプロイするときにサポートされる機能はどれですか。

- A. IPv6
- B. マルチコンテキストモード
- C. レイヤー3ネットワークのユーザー展開
- D. クラスタリング

正解: **C** ([コメントを发表する](#))

質問: **259**

マルチベンダー環境をサポートし、サイト間のトラフィックを保護できるVPNテクノロジーはどれですか？

- A. SSL VPN
- B. VPNを取得
- C. FlexVPN
- D. DMVPN

正解: ([正解を表示します](#))

説明/リファレンス https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

質問: **260**

どのパブリッククラウドプロバイダーがCiscoNextGeneration Firewall Virtualをサポートしていますか？

- A. Google Cloud Platform
- B. Red Hat Enterprise Visualization
- C. VMware ESXi
- D. アマゾンウェブサービス

正解: ([正解を表示します](#))

Cisco Firepower NGFWv in Amazon Web Services (AWS) or Microsoft Azure must be managed by a Cisco Firepower Management Center (FMC) residing in AWS or on-premises. The virtual FCM can be deployed on VMware ESXi, on KVM, and in AWS. Figure 1 shows the various FMC dashboards.

質問: **261**

ネットワークエンジニアがsnmp-serveruserandy myv3 auth sha cisco priv aes 256 cisc0383320506コマンドを入力し、SNMP情報を10.255.254.1のホストに送信する必要があります。この目標を達成するコマンドはどれですか？

- A. 10.255.254.1snmpv3andy内のsnmp-serverホスト
- B. 10.255.254.1バージョン3myv3内のsnmp-serverホスト
- C. 10.255.254.1snmpv3myv3内のsnmp-serverホスト
- D. 10.255.254.1バージョン3andy内のsnmp-serverホスト

正解: (正解を表示します)

説明/リファレンス https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/sm/snmp-server-host.html

質問: 262

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

正解:

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

uses six packets in main mode to establish phase 1

uses three packets in aggressive mode to establish phase 1

IKEv2

standard includes NAT-T

uses four packets to establish phase 1 and phase 2

uses EAP for authenticating remote access clients

質問: 263

2つのDDoS攻撃カテゴリとは何ですか？ 2つ選択してください)

- A. シーケンシャル

- B. プロトコル
- C. データベース
- D. ボリュームベース
- E. 画面ベース

正解: ([正解を表示します](#))

説明説明攻撃には3つの基本的なカテゴリがあります。+大量のトラフィックを使用してネットワーク帯域幅を氾濫させるボリュームベースの攻撃+サーバーリソースの悪用に焦点を当てたプロトコル攻撃+Webアプリケーションに焦点を当てて最も洗練されたと見なされるアプリケーション攻撃深刻なタイプの攻撃参照 <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>説明攻撃には3つの基本的なカテゴリがあります。

+大量のトラフィックを使用してネットワーク帯域幅を氾濫させるボリュームベースの攻撃

+サーバーリソースの悪用に焦点を当てたプロトコル攻撃

説明説明攻撃には3つの基本的なカテゴリがあります。+大量のトラフィックを使用してネットワーク帯域幅を氾濫させるボリュームベースの攻撃+サーバーリソースの悪用に焦点を当てたプロトコル攻撃+Webアプリケーションに焦点を当てて最も洗練されたと見なされるアプリケーション攻撃深刻なタイプの攻撃参照 <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

質問: 264

Cisco AMP for Endpointsは、組織がマルウェアのさまざまなファミリーを検出するのに支援するために何を使用しますか？

- A. ファジーフingerprintを実行するEthos Engine
- B. エンドポイントがクラウドに接続されているときにマルウェアを検出するTetra Engine
- C. 電子メールスキャンを実行するためのClam AV Engine
- D. 動的分析を実行するための機械学習を備えたSpero Engine

正解: A ([コメントを发表する](#))

ETHOSは、シスコのファイルグループ化エンジンです。これにより、ファイルのファミリーをグループ化できるため、マルウェアの亜種が見つかった場合、ETHOSハッシュを悪意のあるものとしてマークし、マルウェアのファミリー全体が即座に検出されます。

ETHOSは、シスコのファイルグループ化エンジンです。これにより、ファイルのファミリーをグループ化できるため、マルウェアの亜種が見つかった場合、ETHOSハッシュを悪意のあるものとしてマークし、マルウェアのファミリー全体が即座に検出されます。

参照：

ETHOS=静的/パッシブヒューリスティックを使用したファジーフingerprint

ETHOSは、シスコのファイルグループ化エンジンです。これにより、ファイルのファミリーをグループ化できるため、マルウェアの亜種が見つかった場合、ETHOSハッシュを悪意のあるものとしてマークし、マルウェアのファミリー全体が即座に検出されます。

ETHOS=静的/パッシブヒューリスティックを使用したファジーフingerprint

質問: 265

。展示を参照してくださいPythonスクリプトが実行されるとどうなりますか？

- A. ホスト名がIPアドレスに変換されて印刷されます。
- B. クライアントのホスト名がクライアントIDフィールドに出力されます。
- C. スクリプトはIPアドレスをFODNIに変換し、それを出力します
- D. スクリプトは、すべてのコンピューターのホスト名をプルして出力します。

正解: ([正解を表示します](#))

質問: 266

ネットワーク管理者は、AMPを備えたCisco ESAを使用して、分析のためにファイルをクラウドにアップロードしています。ネットワークが混雑していて、通信に影響を与えています。Cisco ESAは、分析に必要なファイルをどのように処理しますか。

- A. AMPはSHA-256フィンガープリントを計算してキャッシュし、定期的にアップロードを試みます。
- B. 接続が復元されると、ファイルはアップロードのためにキューに入れられます。
- C. ファイルのアップロードは中止されました。
- D. ESAはすぐにファイルのアップロードを再試行します。

正解: ([正解を表示します](#))

説明

* The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html>

質問: 267

基本的なSYNフラッド攻撃の目的は何ですか？

- A. DNS応答を要求する
- B. バッファをオーバーフローさせる
- C. 接続キューのしきい値制限を超える
- D. レジスタスタックをフラッシュしてバッファを再起動します

正解: ([正解を表示します](#))

質問: 268

AWSパブリッククラウド内にCiscoASAvをデプロイするときにサポートされる機能はどれですか。

- A. マルチコンテキストモード
- B. レイヤー3ネットワークのユーザー展開
- C. IPv6
- D. クラスタリング

正解: ([正解を表示します](#))

AWS上のASAvは、次の機能をサポートします。+次世代のAmazon EC2ComputeOptimizedインスタンスファミリーであるAmazonEC2C5インスタンスのサポート。+仮想プライベートクラウド (VPC)での展開+利用可能な場合は拡張ネットワーキング (SR-IOV)+Amazonマーケットプレイスからの展開+インスタンスあたり最大4つのvCPU+ L3ネットワークのユーザー展開+ルーテッドモード (デフォルト) 注Cisco Adaptive Security仮想アプライアンス (ASAv)は、物理Cisco ASAと同じソフトウェアを実行して、実証済みのセキュリティ機能を仮想フォームファクタで提供します。ASAvはパブリックAWSクラウドにデプロイできます。次に、時間の経過とともに場所を拡大、縮小、またはシフトする仮想および物理データセンターのワークロードを保護するように構成できます。参照 https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96_qsg/asavaws

+次世代のAmazonEC2ComputeOptimizedインスタンスファミリーであるAmazonEC2C5インスタンスのサポート。

+仮想プライベートクラウド (VPC)での展開

+利用可能な場合は拡張ネットワーキング (SR-IOV)

+Amazonマーケットプレイスからのデプロイ

+インスタンスあたり最大4つのvCPU

+L3ネットワークのユーザー展開

+ルーテッドモード (デフォルト)

注 :Cisco Adaptive Security仮想アプライアンス (ASAv)は、物理Cisco ASAと同じソフトウェアを実行して、実証済みのセキュリティ機能を仮想フォームファクタで提供します。ASAvはパブリックAWSクラウドにデプロイできます。

AWS上のASAvは、次の機能をサポートします。+次世代のAmazon EC2ComputeOptimizedインスタンスファミリーであるAmazonEC2C5インスタンスのサポート。+仮想プライベートクラウド (VPC)での展開+利用可能な場合は拡張ネットワーキング (SR-IOV)+Amazonマーケットプレイスからの展開+インスタンスあたり最大4つのvCPU+ L3ネットワークのユーザー展開+ルーテッドモード (デフォルト) 注Cisco Adaptive Security仮想アプライアンス (ASAv)は、物理Cisco ASAと同じソフトウェアを実行して、実証済みのセキュリティ機能を仮想フォームファクタで提供します。ASAvはパブリックAWSクラウドにデプロイできます。次に、時間の経過とともに場所を拡大、縮小、またはシフトする仮想および物理データセンターのワークロードを保護するように構成できます。参照 https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96_qsg/asavaws

質問: 269

組織は、接続が確立される前に悪意のある宛先をブロックすることにより、多層防御を改善しようとしています。ソリューションは、特定のアプリケーションがネットワーク内で使用されるのをブロックできる必要があります。この目標を達成するには、どの製品を使用する必要がありますか？

- A. Cisco Firepower
- B. Cisco Umbrella
- C. ISE
- D. AMP

正解: ([正解を表示します](#))

説明

Cisco Umbrella uses the internet's infrastructure to block malicious destinations before a connection is ever established. Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

質問: 270

管理者は、組織がデバイスの特定のドメインをブロックできるように、CiscoUmbrellaで新しい宛先リストを設定します。domain.comのすべてのサブドメインが確実にブロックされるようにするにはどうすればよいですか？

- A. ブロックリストでdomain.comアドレスを設定します
- B. ブロックリストで*.domain.comアドレスを構成します
- C. ブロックリストで*.comアドレスを設定します。
- D. ブロックリストで*.domain.comアドレスを構成します

正解: ([正解を表示します](#))

質問: 271

透過モードで実行されているCiscoWSAと明示モードで実行されているCiscoWSAの2つの違いは何ですか。2つ選択してください。)

- A. Cisco WSAは、透過モードで実行されている場合にのみ、レイヤ3デバイスを使用してトラフィックをリダイレクトします。
- B. Cisco WSAは、透過モードで実行されている場合にのみ、独自のIPアドレスで応答します。
- C. Cisco WSAは、明示モードで実行されている場合にのみ、独自のIPアドレスで応答します。
- D. Cisco WSAは、透過モードで実行されている場合にのみWebブラウザで設定されます。
- E. Cisco WSAが透過モードで実行されている場合、HTTP要求の宛先としてWSA自身のIPアドレスを使用します。

正解: ([正解を表示します](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **272**

組織の環境にCiscoStealthwatchCloudが導入されています。クラウドロギングは期待どおりに機能していますが、オンプレミスネットワークからログが受信されていません。この問題を解決するには、どのようなアクションを実行しますか？

- A. syslogをCiscoStealthwatchCloudに送信するようにセキュリティアプライアンスを設定します
- B. NetFlowをCiscoStealthwatchCloudに送信するようにセキュリティアプライアンスを設定します
- C. CiscoFTDセンサーを導入してイベントをCiscoStealthwatchCloudに送信します
- D. ネットワークにCisco Stealthwatch Cloudセンサーを導入して、CiscoStealthwatchCloudにデータを送信します

正解: ([正解を表示します](#))

Cisco Stealthwatch Cloudを使用して、組織内のオンプレミスネットワークを監視することもできます。そのためには、少なくとも1つのCisco Stealthwatch Cloud Sensorアプライアンス（仮想または物理アプライアンス）を導入する必要があります。

質問: **273**

CiscoSecurityIntelligenceがCiscoNextGeneration Intrusion Prevention Systemで機能するには、どのライセンスが必要ですか。

- A. URLフィルタリング
- B. コントロール
- C. 保護する
- D. マルウェア

正解: **C** ([コメントを发表する](#))

質問: **274**

ネットワーク管理者は、アクセス制御ポリシーで特定のURLをブロックするルールを構成し、「チャットとインスタントメッセージング」カテゴリを選択しています。この目標を達成するには、どのレピュテーションスコアを選択する必要がありますか？

- A. 1
- B. 3
- C. 5
- D. 10

正解: **D** ([コメントを发表する](#))

「URLカテゴリ」で「チャットとインスタントメッセージング」カテゴリを選択します。

Edit Action

Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info

URL Category

URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)

URL Category Help

Does any URL in the message body or subject belong to one of the selected categories?

Available Categories:

- Advertisements
- Alcohol
- Arts
- Astrology
- Auctions
- Business and Industry
- Chat and Instant Messaging
- Cheating and Plagiarism
- Computer Security
- Computers and Internet

Selected Categories:

- Adult
- Child Abuse Content
- Illegal Activities
- Illegal Downloads
- Illegal Drugs

Use a URL whitelist: ?

Action on URL:

☒ Defang URL ?

☐ Redirect to Cisco Security Proxy ?

☐ Replace URL with text message

Perform Action for:

☒ All messages

☐ Unsigned messages

特定のURLをブロックするには、6から10までのURLレピュテーションを選択する必要があります。

Edit Condition

Message Body or Attachment

Message Body

URL Category

URL Reputation

Message Size

Attachment Content

Attachment File Info

Attachment Protection

Subject Header

Other Header

Envelope Sender

Envelope Recipient

Receiving Listener

Remote IP/Hostname

Reputation Score

URL Reputation

What is the reputation of URL's in the message? This rule evaluates URL's using their Web Based Reputation Score (W

URL Reputation is:

☒ Malicious (-10.0 to -6.0)

☐ Suspect (-5.9 to 5.9)

☐ Clean (6.0 to 10.0)

☐ Custom Range (min to max)

☐ No Score

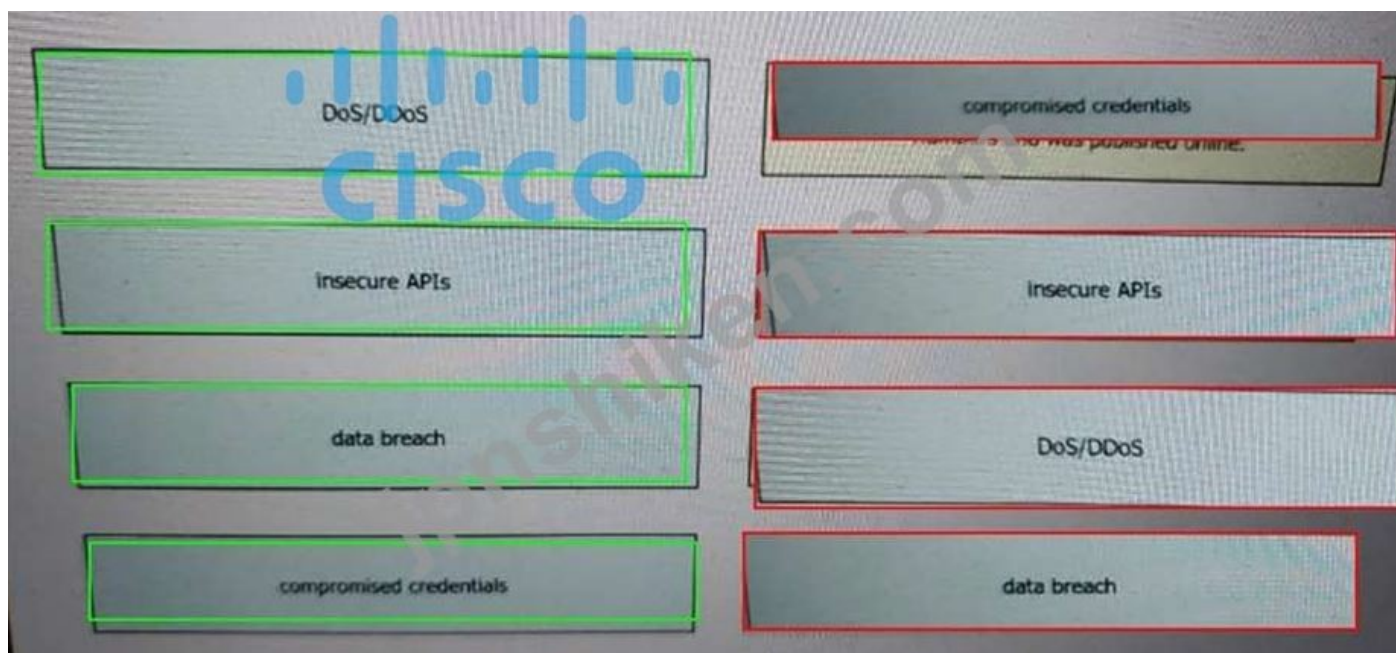
Use a URL whitelist: None ?

質問: 275

脅威を左側から右側の脅威の例にドラッグアンドドロップします

DoS/DDoS	A stolen customer database that contained social security numbers and was published online.
Insecure APIs	A phishing site appearing to be a legitimate login page captures user login information.
data breach	An application attack using botnets from multiple remote locations that flood a web application causing a degraded performance or a complete outage.
compromised credentials	A malicious user gained access to an organization's database from a cloud-based application programming interface that lacked strong authentication controls.

正解:



質問: 276

組織のDMZには2つのシステムがあり、通信のためにそれらの間に暗号化されていないリンクがあります。

組織には定義済みのパスワードポリシーがなく、システムでいくつかのデフォルトアカウントを使用しています。

これらのシステムで使用されているアプリケーションも、厳格なコードレビューを受けていません。攻撃者がブルートフォースでシステムに侵入するのに役立つ脆弱性はどれですか？

- A. 弱いパスワード
- B. 入力検証の欠如
- C. 暗号化がありません
- D. ファイル権限の欠如

正解: ([正解を表示します](#))

バージョン9のエクスポート形式では、テンプレートを使用して、柔軟かつ拡張可能な方法でIPパケットフローの監視にアクセスできます。テンプレートは、構造とセマンティクスの対応する説明とともに、フィールドのコレクションを定義します。

バージョン9のエクスポート形式では、テンプレートを使用して、柔軟かつ拡張可能な方法でIPパケットフローの監視にアクセスできます。テンプレートは、構造とセマンティクスの対応する説明とともに、フィールドのコレクションを定義します。

参照：

バージョン9のエクスポート形式では、テンプレートを使用して、柔軟かつ拡張可能な方法でIPパケットフローの監視にアクセスできます。テンプレートは、構造とセマンティクスの対応する説明とともに、フィールドのコレクションを定義します。

質問: 277

SDNノースバウンドAPIの2つの機能は何ですか？ (2つ選択してください。)

- A. ノースバウンドAPIは、アプリケーションがネットワークを動的に構成するためのプログラム可能なインターフェースを提供します。
- B. ノースバウンドAPIは、SDNコントローラーとビジネスアプリケーション間のインターフェースを形成します。
- C. ノースバウンドAPIは、SDNコントローラーとネットワークスイッチまたはルーター間のインターフェースを形成します。
- D. OpenFlowは標準化されたノースバウンドAPIプロトコルです。
- E. ノースバウンドAPIは、NETCONFプロトコルを使用してアプリケーションと通信します。

正解: ([正解を表示します](#))

質問: 278

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

正解:

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

uses six packets in main mode to establish phase 1

uses three packets in aggressive mode to establish phase 1

IKEv2

standard includes NAT-T

uses four packets to establish phase 1 and phase 2

uses EAP for authenticating remote access clients

質問: 279

展示を参照してください。

```
Sysauthcontrol          Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                        = AUTHENTICATOR
PortControl                = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                   = SINGLE_HOST
QuietPeriod                = 60
ServerTimeout              = 0
SuppTimeout                = 30
ReAuthMax                  = 2
MaxReq                     = 2
TxPeriod                   = 30
```



この出力を表示するために使用されたコマンドはどれですか？

- A. dot1xのすべての概要を表示
- B. dot1xを表示
- C. dot1xallを表示
- D. show dot1x interface gi1 / 0/12

正解: C ([コメントを發表する](#))

質問: 280

管理者がインターネットアクセスを必要とせずにエアギャップサイトにKubernetesクラスターをデプロイできるセキュリティ製品はどれですか。

- A. Ciscoクラウドプラットフォーム
- B. Cisco Container Controller
- C. Cisco Container Platform
- D. Ciscoコンテンツプラットフォーム

正解: C ([コメントを發表する](#))

質問: 281

SNMPプルに対するネットワークテレメトリの利点は何ですか？

- A. セキュリティ
- B. 精度
- C. スケーラビリティ
- D. カプセル化

正解: ([正解を表示します](#))

質問: 282

構成されたポスチャポリシー要件が満たされていない場合、どのコンプライアンスステータスが表示されますか？

- A. 不明
- B. 準拠
- C. 非準拠
- D. 承認済み

正解: ([正解を表示します](#))

質問: 283

オンプレミスではない環境での侵害、アプリケーションリスク、およびデータ侵害を削減するのに役立つCiscoAPIベースのブローカとは何ですか。

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco AMP
- D. Cisco App Dynamics

正解: ([正解を表示します](#))

Cisco Cloudlock is the API-based cloud access security broker (CASB) that helps accelerate use of the cloud. By securing your identities, data, and apps, Cloudlock combats account compromises, breaches, and cloud app ecosystem risks. Our API-driven approach provides a simple and open way to enable healthy cloud adoption.

質問: 284

Cisco Threat Intelligence Directorと統合して、セキュリティの脅威に関する情報を提供し、SOCがそれらの脅威への対応をプロアクティブに自動化できるようにするものは何ですか。

- A. Cisco Stealthwatch
- B. Cisco Threat Grid
- C. 外部脅威フィード
- D. Cisco Umbrella

正解: ([正解を表示します](#))

質問: 285

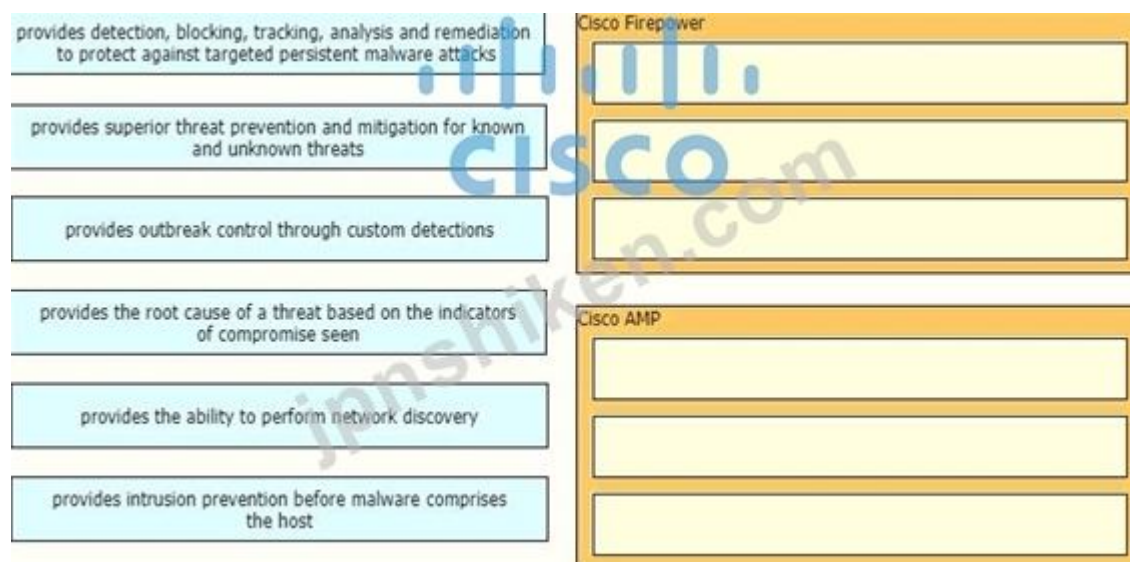
ACME-Router (config)#loginブロックの結果は何ですか-CiscdOSルータでの60コマンド内での100回の試行4の場合？

- A. ログインに4回失敗すると、回線は60秒間ブロックされ、ACL1では許可IPアドレスのみが許可されます。
- B. ログインに4回失敗すると、回線は100秒間ブロックされ、ACLで許可されるIPアドレスのみが許可されます。
- C. 60秒間に4つの障害が発生した場合、ルータは100秒間クワイエットモードになります。
- D. 4回のログイン試行が100秒以内に失敗した場合、次のログインプロンプトまで60秒待ちます。

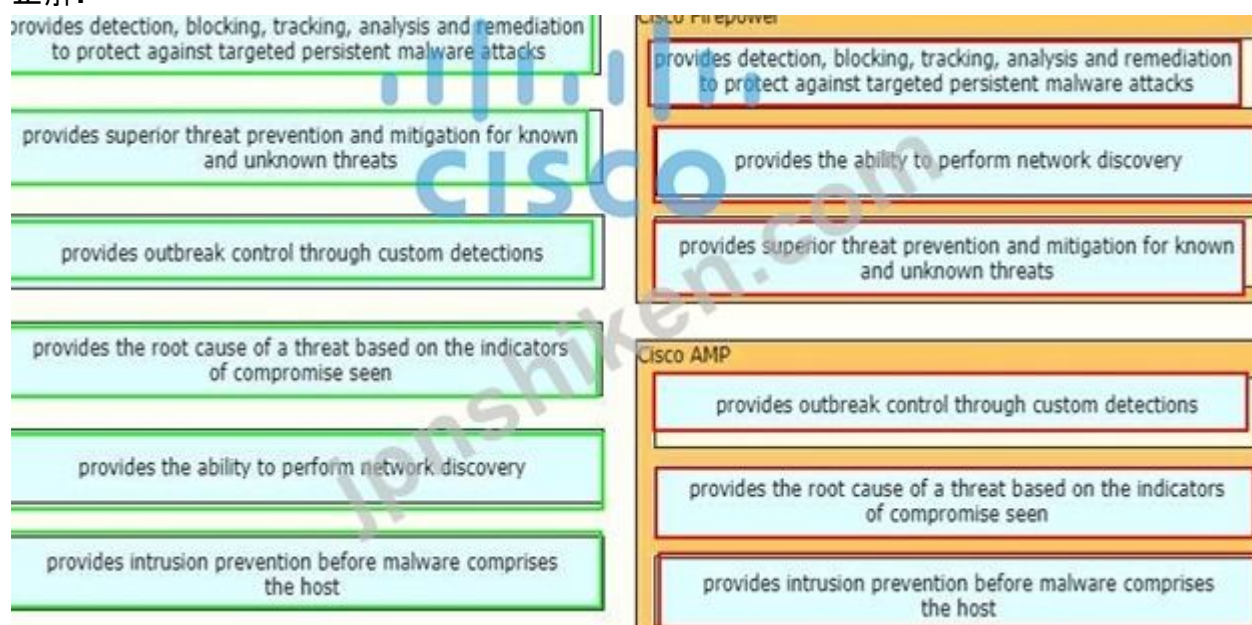
正解: ([正解を表示します](#))

質問: 286

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。



正解:



説明Firepowerシステムは、ネットワーク検出およびIDポリシーを使用して、ネットワーク上のトラフィックのホスト、アプリケーション、およびユーザーデータを収集します。特定の種類の検出およびIDデータを使用して、ネットワーク資産の包括的なマップを構築し、フォレンジック分析、動作プロファイリング、アクセス制御を実行し、組織が影響を受けやすい脆弱性とエクスプロイトを軽減および対応できます。Cisco Advanced Malware Protection (AMP) ソリューションを使用すると、マルウェアを検出してブロックし、マルウェアを継続的に分析して、遡及的なアラートを受け取ることができます。AMP for Networksは、ポイントインタイム検出を超えて、攻撃の前、最中、後の攻撃の連続体全体にわたって組織を保護する、ネットワークベースの高度なマルウェア保護を提供します。Cisco Firepowerネットワーク脅威アプライアンス向けに設計されており、AMP for Networksは、単一のシステム内の複数の脅威ベクトルにわたるマルウェアの脅威を検出、ブロック、追跡、および封じ込めます。また、高度に洗練された、ターゲットを絞った、ゼロデイで永続的な高度なマルウェアの脅威から組織を保護するために必要な可視性と制御を提供します。

有効的な**350-701**問題集はJPNTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTest.comは今最新**350-701**試験問題集を提供します。JPNTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%**ディスカウント、特別な割引コード: **JPNshiken**」

質問: 287

Cisco Advanced Phishing Protectionはどのようにユーザーを保護しますか？

- A. DKIMを使用して送信者を検証します。
- B. 送信者がどのIDを認識するかを決定します
- C. 機械学習とリアルタイムの行動分析を使用します。
- D. メッセージを安全に送信するセンサーを利用しています。

正解: ([正解を表示します](#))

・ Determines which identities the recipient perceives is sending the message

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf>

質問: 288

CiscoルータでNetflowエクスポートを設定するときに必要なパラメータはどれですか。

- A. DSCP値
- B. ソースインターフェース
- C. エクスポート名
- D. エクスポートの説明

正解: ([正解を表示します](#))

NetFlowエクスポートを設定する例を以下に示します。

フローエクスポートエクスポート

宛先192.168.100.22

トランスポートUDP2055

質問: 289

Cisco AMP for Endpointsは、組織がマルウェアのさまざまなファミリーを検出するのに支援するために何を使用しますか？

- A. ファジーフィンガープリントを実行するEthos Engine
- B. エンドポイントがクラウドに接続されているときにマルウェアを検出するTetra Engine
- C. 電子メールスキャンを実行するためのClam AV Engine
- D. 動的分析を実行するための機械学習を備えたSpero Engine

正解: ([正解を表示します](#))

説明

ETHOSは、シスコのファイルグループ化エンジンです。これにより、ファイルのファミリーをグループ化できるため、マルウェアの亜種が見つかった場合、ETHOSハッシュを悪意のあるものとしてマークし、マルウェアのファミリー全体が即座に検出されます。

参照：

ETHOS=静的/パッシブヒューリスティックを使用したファジーフィンガープリント

質問: 290

エンジニアがCiscoUmbrellaを設定しており、2つの異なるポリシーを参照するIDを持っています。.....使用が2番目の使用よりも優先されることを保証するアクションはどれですか？

- A. ポリシーの順序で最初に正しいポリシーを作成します。

- B. 最後に変更されたタイムスタンプを持つポリシーのみを構成します。
- C. 最も具体的な構成のポリシーをポリシーの順序の最後に配置します。
- D. 要求を正しいポリシーにリダイレクトするようにデフォルトのポリシーを構成します。
- 正解: [\(正解を表示します\)](#)

質問: 291

NetFlowエクスポートフォーマットを左から右の説明にドラッグアンドドロップします。

Version 1	appropriate only for the main cache
Version 5	introduced support for aggregation caches
Version 8	appropriate only for legacy systems
Version 9	introduced extensibility

正解:

Version 1	Version 1
Version 5	Version 5
Version 8	Version 9
Version 9	Version 8

質問: 292

IOSゾーンベースのファイアウォールに関する正しい説明はどれですか。

- A. 割り当てられていないインターフェースは割り当てられたインターフェースと通信できます
- B. ゾーンに割り当てることができるインターフェースは1つだけです。
- C. インターフェースを複数のゾーンに割り当てることができます。
- D. インターフェースは1つのゾーンにのみ割り当てることができます。

正解: D [\(コメントを发表する\)](#)

説明/リファレンス <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

質問: 293

エンジニアは既存のMicrosoftOffice365環境にCiscoCESを実装しており、受信メールをCisco CEにルーティングする必要があります。このタスクを実行するには、レコードを変更する必要がありますか。

- A. DKIM
- B. SPF
- C. CNAME
- D. MX

正解: ([正解を表示します](#))

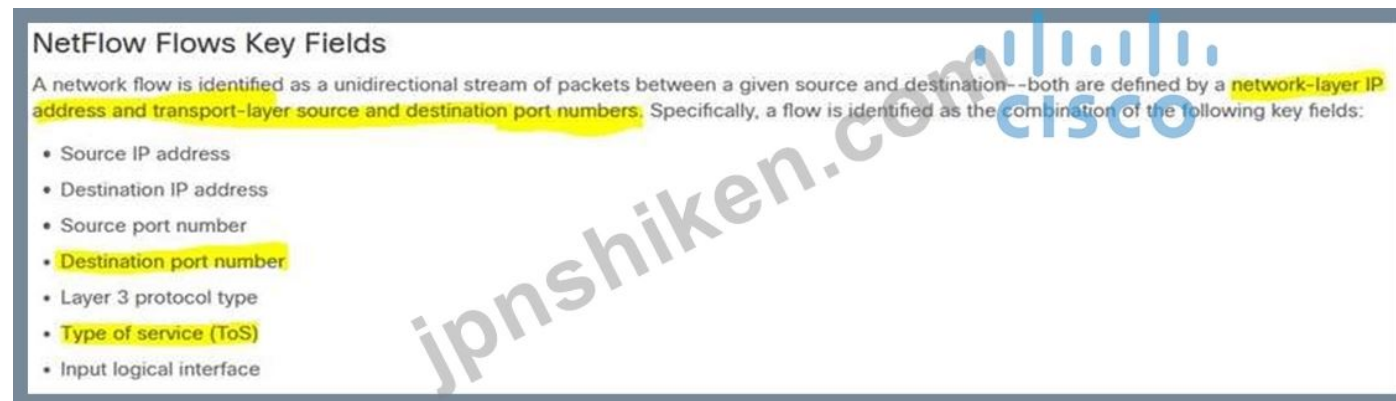
質問: 294

NetFlowフローで定義されている2つのフィールドはどれですか？{2つ選択してください。}

- A. サービスバイトのタイプ
- B. レイヤー4プロトコルタイプ
- C. サービスクラスビット
- D. 出力論理インターフェース
- E. 宛先ポート

正解: ([正解を表示します](#))

参照 :



質問: 295

クロスサイトスクリプティングとSQLインジェクション、攻撃の違いは何ですか？

- A. クロスサイトスクリプティングは、コードがデータベースに挿入される攻撃ですが、SQLインジェクションは、コードがブラウザーに挿入される攻撃です。
- B. クロスサイトスクリプティングはリモートサイトを標的としたブルートフォース攻撃ですが、SQLインジェクションはソーシャルエンジニアリング攻撃です。
- C. クロスサイトスクリプティングは企業の幹部が攻撃されるときですが、SQLインジェクションはデータベースが操作されるときです。
- D. クロスサイトスクリプティングは、コードがサーバー側から実行される攻撃ですが、SQLインジェクションは、コードがクライアント側から実行される攻撃です。

正解: ([正解を表示します](#))

説明

クロスサイトスクリプティング (XSS)はブルートフォース攻撃ではないため、回答Bは正しくありません。

「クロスサイトスクリプティングは企業の幹部が攻撃されたときです」という記述は正しくないため、回答Cは正しくありません。XSSは、他のアプリケーションユーザーを標的とするクライアント側の脆弱性です。

「クロスサイトスクリプティングはサーバー側からコードが実行される攻撃である」という記述があるため、回答Dは正しくありません。実際、XSSは、クライアント側で実行されるスクリプトを挿入することにより、Webサイトの脆弱性を悪用する方法です。

したがって、回答Aのみが残ります。XSSでは、攻撃者は自分の悪意のあるコード（通常は悪意のあるリンク）をデータベースに挿入しようとします。他のユーザーが自分のリンクをたどると、攻撃者がデータを盗むことができるWebサイトにWebブラウザがリダイレクトされます。SQLインジェクションでは、攻撃者は（ブラウザを介して）SQLコードを、GET / POSTパラメータのデータサニタイズまたは検証メソッドを使用しないフォーム、Cookie、またはHTTPヘッダーに挿入しようとします。

注 :SQLインジェクション攻撃とXSSインジェクション攻撃の主な違いは、SQLインジェクション攻撃はデータベースから情報を盗むために使用されるのに対し、XSS攻撃は、攻撃者がデータを盗むことができるWebサイトにユーザーをリダイレクトするために使用されることです。

質問: 296

CoAが発行されるのはどの2つの状況ですか？ 2つ選択してください)

- A. 新しい認証ルールがポリシーサービスノードのポリシーに追加されました。
- B. IdentityServiceEngineサーバーでエンドポイントが削除されました。
- C. 新しいIDソースシーケンスが作成され、認証ポリシーで参照されます。
- D. エンドポイントが初めてプロファイルされます。
- E. 新しいIdentityServiceEngineサーバーが管理ペルソナとともに展開に追加されます

正解: ([正解を表示します](#))

プロファイリングサービスは、次の場合に許可の変更を発行します。

-エンドポイントが削除されました-エンドポイントが[エンドポイント]ページから削除され、エンドポイントがネットワークから切断または削除された場合。

例外アクションが構成されているプロファイルごとに構成されている例外アクションがあり、そのエンドポイントからの異常なイベントまたは許容できないイベントが発生する場合。プロファイリングサービスは、CoAを発行して、エンドポイントに対応する静的プロファイルに移動します。

-エンドポイントが初めてプロファイリングされるエンドポイントが静的に割り当てられ、初めてプロファイリングされない場合。たとえば、プロファイルが不明から既知のプロファイルに変更されます。

+エンドポイントIDグループが変更された承認ポリシーで使用するエンドポイントIDグループにエンドポイントが追加または削除された場合。

プロファイリングサービスは、エンドポイントIDグループに変更があった場合に、CoAを発行します。エンドポイントIDグループは、次の許可ポリシーで使用されます。

++エンドポイントが動的にプロファイリングされると、エンドポイントIDグループが変更されます++動的エンドポイントに対して静的割り当てフラグがtrueに設定されると、エンドポイントIDグループが変更されます-エンドポイントプロファイリングポリシーが変更され、そのポリシーが許可ポリシーで使用されます-エンドポイントプロファイリングポリシーが変更され、そのポリシーが許可ポリシーで使用される論理プロファイルに含まれている場合。エンドポイントプロファイリングポリシーは、プロファイリングポリシーの一致により、またはエンドポイントが論理プロファイルに関連付けられているエンドポイントプロファイリングポリシーに静的に割り当てられている場合に変更される可能性があります。どちらの場合も、エンドポイントプロファイリングポリシーが許可ポリシーで使用されている場合にのみ、プロファイリングサービスがCoAを発行します。参照：

<https://www.cisco.com>。

++動的エンドポイントの静的割り当てフラグがtrueに設定されている場合、エンドポイントIDグループが変更されます-エンドポイントプロファイリングポリシーが変更され、そのポリシーが許可ポリシーで使用されている場合-エンドポイントプロファイリングポリシーが変更され、ポリシーが許可ポリシーで使用される論理プロファイル。エンドポイントプロファイリングポリシーは、プロファイリングポリシーの一致により、またはエンドポイントが論理プロファイルに関連付けられているエンドポイントプロファイリングポリシーに静的に割り当てられている場合に変更される可能性があります。どちらの場合も、エンドポイントプロファイリングポリシーが許可ポリシーで使用されている場合にのみ、プロファイリングサービスがCoAを発行します。

参照：

++エンドポイントが動的にプロファイリングされると、エンドポイントIDグループが変更されます++動的エンドポイントに対して静的割り当てフラグがtrueに設定されると、エンドポイントIDグループが変更されますエンドポイントプロファイリングポリシーが変更され、そのポリシーが許可ポリシーで使用されますエンドポイントプロファイリングポリシーが変更され、そのポリシーが許可ポリシーで使用する論理プロファイルに含まれている場合。エンドポイントプロファイリングポリシーは、プロファイリングポリシーの一致により、またはエンドポイントが論理プロファイルに関連付けられているエンドポイントプロファイリングポリシーに静的に割り当てられている場合に変更される可能性があります。どちらの場合も、エンドポイントプロファイリングポリシーが許可ポリシーで使用されている場合にのみ、プロファイリングサービスがCoAを発行します。参照：
<https://www.cisco.com>。

質問: 297

マルチベンダー環境をサポートし、サイト間のトラフィックを保護できるVPNテクノロジーはどれですか？

- A. SSL VPN
- B. VPNを取得
- C. FlexVPN
- D. DMVPN

正解: C ([コメントを發表する](#))

FlexVPNはIKEv2ベースのVPNテクノロジーであり、従来のサイト間VPN実装を超えるいくつかの利点を提供します。FlexVPNは、Cisco以外のIKEv2実装と相互運用できる標準ベースのソリューションです。したがって、FlexVPNはマルチベンダー環境をサポートできます。3つのVPNテクノロジーはすべて、サイト間のトラフィック（サイト間またはスポークツースポーク）をサポートします。

質問: 298

楕円曲線暗号は、現在のどの暗号化技術に取って代わることを目的とした、より強力でより効率的な暗号法ですか？

- A. 3DES
- B. RSA
- C. DES
- D. AES

正解: ([正解を表示します](#))

説明

今日インターネットで普及している公開鍵暗号であるRSAと比較すると、楕円曲線暗号（ECC）は、キーサイズが小さく、計算が高速で、メモリ、エネルギー、帯域幅を節約できるため、小型デバイスに適しています。

質問: 299

承認済みCiscoISEサーバとADドメインを統合する場合の前提条件は何ですか。

- A. 共通のDNSサーバを構成します。
- B. CiscoISEサーバとADサーバを同じサブネットに配置します。
- C. CiscoISEサーバとADサーバのドックを同期します
- D. 共通の管理者アカウントを設定します。

正解: C ([コメントを發表する](#))

質問: 300

CiscoASDMよりもCiscoFMCを使用する利点は何ですか。

- A. Cisco FMCはJavaを使用し、CiscoASDMはHTML5を使用します。
 - B. Cisco FMCは集中管理を提供しますが、CiscoASDMは提供しません。
 - C. Cisco FMCはデバイスへの設定のプッシュをサポートしていますが、CiscoASDMはサポートしていません。
 - D. Cisco FMCはすべてのファイアウォール製品をサポートしますが、CiscoASDMはCiscoASAデバイスのみをサポートします
- 正解: **D** ([コメントを发表する](#))

<https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>

質問: **301**

NetFlowフローモニタリングの2つの機能は何ですか？ 2つ選択してください

- A. 入力および出力情報を追跡できます
- B. フローレコードとフローインポーターを含める
- C. すべての入力フロー情報をインターフェースにコピーします
- D. インターフェイスでのパケットサンプリングは必要ありません
- E. マルチキャスト、MPLS、またはブリッジトラフィックの追跡に使用できます

正解: ([正解を表示します](#))

以下は、FlexibleNetFlowの制限事項です。

- +従来のNetFlow (NF) アカウンティングはサポートされていません。
- +フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。
- +入力と出力の両方のNetFlowアカウンティングがサポートされています。
- + Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。
- +インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。

以下は、FlexibleNetFlowの制限事項です。

- +従来のNetFlow (NF) アカウンティングはサポートされていません。
- +フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。
- +入力と出力の両方のNetFlowアカウンティングがサポートされています。
- + Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。
- +インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。

参照：

[Consolidated_guide / b_consolidated_3850_3se_cg_chapter_011010.html](#)

NetFlowを設定するときは、次のガイドラインと制限に従ってください。

- + PFC3Aモードを除いて、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。
- +NetFlowはマルチキャストIPトラフィックをサポートします。
- フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、VPNのあるサイトから同じVPNの別のサイトにサービスプロバイダーバックボーンを通過するMPLSVPNIPフローをキャプチャできます。FlexibleNetFlowの制限は次のとおりです。
- +従来のNetFlow (NF) アカウンティングはサポートされていません。
- +フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。
- +入力と出力の両方のNetFlowアカウンティングがサポートされています。

+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。

+ インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。

Consolidated_guide / b_consolidated_3850_3se_cg_chapter_011010.html

NetFlowを設定するときは、次のガイドラインと制限に従ってください。

+ PFC3Aモードを除いて、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。

+ NetFlowはマルチキャストIPトラフィックをサポートします。

フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、VPNのあるサイトから同じVPNの別のサイトにサービスプロバイダーバックボーンを通過するMPLS VPNIPフローをキャプチャできま

す。solidated_guide/b_consolidated_3850_3se_cg_chapter_011010.htmlNetFlowを設定するときは、次のガイドラインと制限に従ってください。

+ PFC3Aモードを除いて、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。

+ NetFlowはマルチキャストIPトラフィックをサポートします。

フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、VPNのあるサイトから同じVPNの別のサイトにサービスプロバイダーバックボーンを通過するMPLSVPNIPフローをキャプチャできます。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **302**

Cisco Workload Optimization Managerは、アプリケーションのパフォーマンスの問題を軽減するのにどのように役立ちますか。

A. AWSLambdaシステムをデプロイします

B. 流路を最適化します

C. ワークロードフォレンジックスコアを設定します

D. リソースのサイズ変更を自動化します。

正解: ([正解を表示します](#))

質問: **303**

ネットワークリソースにアクセスするために、証明書を展開し、モバイルデバイスにサブリカントを構成するために使用される方法はどれですか。

A. 搭乗中のBYOD

B. 単純な証明書登録プロトコル

C. クライアントプロビジョニング

D. MAC認証バイパス

正解: ([正解を表示します](#))

企業ネットワークで個人用デバイスをサポートする場合は、ユーザー（従業員 請負業者、ゲスト）とそのデバイスを認証および承認することにより、ネットワークサービスと企業データを保護する必要があります。Cisco ISEは、従業員が企業ネットワーク上でパーソナルデバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ネイティブサプリカントプロビジョニング ネットワークセットアップアシスタント)を実行するか、デバイスをマイデバイスポータルに追加することにより、個人のデバイスをネットワークに追加できます。

ネイティブサプリカントプロファイルはすべてのデバイスで利用できるわけではないため、ユーザーはマイデバイスポータルを使用してこれらのデバイスを手動で追加できます。または、Bring Your Own Device (BYOD)ルールを構成して、これらのデバイスを登録することもできます。

企業ネットワークで個人用デバイスをサポートする場合は、ユーザー（従業員 請負業者、ゲスト）とそのデバイスを認証および承認することにより、ネットワークサービスと企業データを保護する必要があります。Cisco ISEは、従業員が企業ネットワーク上でパーソナルデバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ネイティブサプリカントプロビジョニング ネットワークセットアップアシスタント)を実行するか、デバイスをマイデバイスポータルに追加することにより、個人のデバイスをネットワークに追加できます。

ネイティブサプリカントプロファイルはすべてのデバイスで利用できるわけではないため、ユーザーはマイデバイスポータルを使用してこれらのデバイスを手動で追加できます。または、Bring Your Own Device (BYOD)ルールを構成して、これらのデバイスを登録することもできます。

企業ネットワークで個人用デバイスをサポートする場合は、ユーザー（従業員 請負業者、ゲスト）とそのデバイスを認証および承認することにより、ネットワークサービスと企業データを保護する必要があります。Cisco ISEは、従業員が企業ネットワーク上でパーソナルデバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ネイティブサプリカントプロビジョニング ネットワークセットアップアシスタント)を実行するか、デバイスをマイデバイスポータルに追加することにより、個人のデバイスをネットワークに追加できます。

ネイティブサプリカントプロファイルはすべてのデバイスで利用できるわけではないため、ユーザーはマイデバイスポータルを使用してこれらのデバイスを手動で追加できます。または、Bring Your Own Device (BYOD)ルールを構成して、これらのデバイスを登録することもできます。

参照：

m_ise_devices_byod.html

m_ise_devices_byod.html

質問: 304

エンジニアは、ネットワーク内のCiscoスイッチで802.1X認証を設定し、メカニズムとしてCoAを使用しています。CoAトラフィックがネットワークを通過できるようにするには、ファイアウォールのどのポートを開く必要がありますか？

A. TCP 6514

B. UDP 1700

C. TCP 49

D. UDP 1812

正解: ([正解を表示します](#))

説明

説明

CoAメッセージは、プラットフォームに応じて2つの異なるudpポートで送信されます。シスコはUDPポートで標準化1700、実際のRFCはUDPポート3799を使用して呼び出します。

質問: 305

SDNサウスバウンドAPIプロトコルの機能は何ですか？

- A. コントローラーが変更を行えるようにする
- B. コントロールプレーンアプリケーションの動的構成を可能にするため
- C. コントローラーがRESTを使用できるようにします
- D. コントロールプレーンアプリケーションの静的構成を可能にするため

正解: [\(正解を表示します\)](#)

説明

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs.

質問: 306

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides the ability to perform network discovery

provides intrusion prevention before malware comprises the host

Cisco Firepower

Cisco AMP

正解:

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides the ability to perform network discovery

provides intrusion prevention before malware comprises the host

Cisco Firepower

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides the ability to perform network discovery

provides superior threat prevention and mitigation for known and unknown threats

Cisco AMP

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides intrusion prevention before malware comprises the host

質問: 307

エンジニアは、トラフィックを監視し、イベントに基づいてインシデントを作成し、APIを介して他のクラウドソリューションと統合するクラウドソリューションを必要としています。この目標を達成するには、どのソリューションを使用する必要がありますか？

- A. SIEM
- B. CASB
- C. アダプティブMFA
- D. Cisco Cloudlock

正解: ([正解を表示します](#))

+ Cisco Cloudlockは、クラウドデータ損失防止 (DLP) エンジンを使用してクラウド環境を継続的に監視し、ポリシーに違反してクラウド環境に保存されている機密情報を特定します。+CloudlockはAPIベースです。+インシデントは、CiscoCloudlockアプリケーションの重要なリソースです。これらは、ポリシー検出基準によってオブジェクト (ドキュメント、フィールド、フォルダー、投稿、またはファイル) が一致したときに、Cloudlockポリシーエンジンによってトリガーされます。参照 <https://docs.umbrella.com/cloudlock-documentation/docs/endpoints>注 +セキュリティ情報およびイベント管理 (SIEM) プラットフォームは、セキュリティシステム、ネットワーク、およびコンピューターからログおよびイベントデータを収集し、実用的なセキュリティに変換します洞察。+インシデントは、アラートポリシーのトリガーの記録です。

ポリシーに違反してクラウド環境に保存されている機密情報を特定するため。

+CloudlockはAPIベースです。

+インシデントは、CiscoCloudlockアプリケーションの重要なリソースです。これらは、ポリシー検出基準によってオブジェクト (ドキュメント、フィールド、フォルダー、投稿、またはファイル) が一致したときに、Cloudlockポリシーエンジンによってトリガーされます。

参照：

ノート：

+セキュリティ情報およびイベント管理 (SIEM) プラットフォームは、セキュリティシステム、ネットワーク、およびコンピューターからログおよびイベントデータを収集し、それを実用的なセキュリティインサイトに変換します。

+インシデントは、アラートポリシーのトリガーの記録です。Cloud Monitoringは、次の場合にインシデントを開きます。

+ Cisco Cloudlockは、クラウドデータ損失防止 (DLP) エンジンを使用してクラウド環境を継続的に監視し、ポリシーに違反してクラウド環境に保存されている機密情報を特定します。+CloudlockはAPIベースです。+インシデントは、CiscoCloudlockアプリケーションの重要なリソースです。これらは、ポリシー検出基準によってオブジェクト (ドキュメント、フィールド、フォルダー、投稿、またはファイル) が一致したときに、Cloudlockポリシーエンジンによってトリガーされます。参照 <https://docs.umbrella.com/cloudlock-documentation/docs/endpoints>注 +セキュリティ情報およびイベント管理 (SIEM) プラットフォームは、セキュリティシステム、ネットワーク、およびコンピューターからログおよびイベントデータを収集し、実用的なセキュリティに変換します洞察。+インシデントは、アラートポリシーのトリガーの記録です。

質問: 308

組織は、接続が確立される前に悪意のある宛先をブロックすることにより、多層防御を改善しようとしています。ソリューションは、特定のアプリケーションがネットワーク内で使用されるのをブロックできる必要があります。この目標を達成するには、どの製品を使用する必要がありますか？

- A. Cisco Firepower
- B. Cisco Umbrella
- C. ISE
- D. AMP

正解: ([正解を表示します](#))

説明

Cisco Umbrella uses the internet's infrastructure to block malicious destinations before a connection is ever established. Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

質問: 309

Cisco DNA Centerの2つの機能のうち、ソフトウェア定義ネットワークソリューションで使用されているものはどれですか。2つ選択してください

- A. 会計
- B. 保証
- C. 自動化
- D. 認証
- E. 暗号化

正解: ([正解を表示します](#))

CiscoDNACenterでできること

自動化：単一のダッシュボードを使用してネットワークを管理および自動化することにより、時間を節約します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。

安全なポリシー :ビジネスニーズに基づいて、グループベースの安全なアクセスとネットワークセグメンテーションを展開します。Cisco DNA Centerを使用すると、ネットワークデバイスではなく、ユーザとアプリケーションにポリシーを適用できます。自動化により、手動操作と人的エラーに関連するコストが削減され、稼働時間の増加とセキュリティの向上が実現します。次に、Assuranceはネットワークを評価し、コンテキストを使用してデータをインテリジェンスに変換し、ネットワークデバイスポリシーの変更が意図を達成していることを確認します。

保証 :ネットワークとワイヤレスの状態の変化をリアルタイムで監視、識別、対応します。Cisco DNA Centerは、ネットワークの有線および無線デバイスを使用してあらゆる場所にセンサーを作成し、実際のネットワーク状態に基づいてリアルタイムのフィードバックを提供します。Cisco DNA Assuranceエンジンは、ネットワークセンサーの洞察をストリーミングテレメトリと関連付け、これをこれらのデータソースの現在のコンテキストと比較します。Cisco DNA Centerダッシュボードでヘルススコアをすばやく確認すると、パフォーマンスの問題がある場所を確認し、最も可能性の高い原因を数分で特定できます。

エコシステムの拡張：新しいCisco DNA Centerプラットフォームにより、ITはCisco®ソリューションとサードパーティテクノロジーを単一のネットワークオペレーションに統合して、ITワークフローを合理化し、ビジネス価値とイノベーションを向上させることができます。Cisco DNA Centerを使用すると、ITおよびビジネスアプリケーションとのオープンインターフェイスでネットワークを実行し、IT運用およびテクノロジードメイン間で統合し、異種ネットワークデバイスを管理できます。

CiscoDNACenterでできること

自動化：単一のダッシュボードを使用してネットワークを管理および自動化することにより、時間を節約します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。

安全なポリシー :ビジネスニーズに基づいて、グループベースの安全なアクセスとネットワークセグメンテーションを展開します。Cisco DNA Centerを使用すると、ネットワークデバイスではなく、ユーザとアプリケーションにポリシーを適用できます。自動化により、手動操作と人的エラーに関連するコストが削減され、稼働時間の増加とセキュリティの向上が実現します。次に、Assuranceはネットワークを評価し、コンテキストを使用してデータをインテリジェンスに変換し、ネットワークデバイスポリシーの変更が意図を達成していることを確認します。

保証 :ネットワークとワイヤレスの状態の変化をリアルタイムで監視、識別、対応します。Cisco DNA Centerは、ネットワークの有線および無線デバイスを使用してあらゆる場所にセンサーを作成し、実際のネットワーク状態に基づいてリアルタイムのフィードバックを提供します。Cisco DNA Assuranceエンジンは、ネットワークセンサーの洞察をストリーミングテレメトリと関連付け、これをこれらのデータソースの現在のコンテキストと比較します。Cisco DNA Centerダッシュボードでヘルススコアをすばやく確認すると、パフォーマンスの問題がある場所を確認し、最も可能性の高い原因を数分で特定できます。

エコシステムの拡張：新しいCisco DNA Centerプラットフォームにより、ITはCisco®ソリューションとサードパーティテクノロジーを単一のネットワークオペレーションに統合して、ITワークフローを合理化し、ビジネス価値とイノベーションを向上させることができます。Cisco DNA Centerを使用すると、ITおよびビジネスアプリケーションとのオープンインターフェイスでネットワークを実行し、IT運用およびテクノロジードメイン間で統合し、異種ネットワークデバイスを管理できます。

参照：

CiscoDNACenterでできること

自動化：単一のダッシュボードを使用してネットワークを管理および自動化することにより、時間を節約します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。

安全なポリシー：ビジネスニーズに基づいて、グループベースの安全なアクセスとネットワークセグメンテーションを展開します。Cisco DNA Centerを使用すると、ネットワークデバイスではなく、ユーザとアプリケーションにポリシーを適用できます。自動化により、手動操作と人的エラーに関連するコストが削減され、稼働時間の増加とセキュリティの向上が実現します。次に、Assuranceはネットワークを評価し、コンテキストを使用してデータをインテリジェンスに変換し、ネットワークデバイスポリシーの変更が意図を達成していることを確認します。

保証：ネットワークとワイヤレスの状態の変化をリアルタイムで監視、識別、対応します。Cisco DNA Centerは、ネットワークの有線および無線デバイスを使用してあらゆる場所にセンサーを作成し、実際のネットワーク状態に基づいてリアルタイムのフィードバックを提供します。Cisco DNA Assuranceエンジンは、ネットワークセンサーの洞察をストリーミングテレメトリと関連付け、これをこれらのデータソースの現在のコンテキストと比較します。Cisco DNA Centerダッシュボードでヘルススコアをすばやく確認すると、パフォーマンスの問題がある場所を確認し、最も可能性の高い原因を数分で特定できます。

エコシステムの拡張：新しいCisco DNA Centerプラットフォームにより、ITはCisco®ソリューションとサードパーティテクノロジーを単一のネットワークオペレーションに統合して、ITワークフローを合理化し、ビジネス価値とイノベーションを向上させることができます。Cisco DNA Centerを使用すると、ITおよびビジネスアプリケーションとのオープンインターフェイスでネットワークを実行し、IT運用およびテクノロジードメイン間で統合し、異種ネットワークデバイスを管理できます。

質問: 310

ソフトウェア定義のネットワークアーキテクチャ内のコントローラーがネットワーク内のスイッチの構成を動的に変更する場合、どのタイプのAPIが使用されますか？

A. 西行きAP

B. サウスバウンドAPI

C. ノースバウンドAPI

D. イーストバウンドAPI

正解: ([正解を表示します](#))

サウスバウンドAPIを使用すると、SDNコントローラーはリアルタイムの要求とスケーラビリティのニーズに基づいて動的に変更を加えることができます。



質問: 311

展示を参照してください。

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
                      snmp_ro_community, snmp_rw_community,
                      snmp_retry, snmp_timeout,
                      cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
        'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}dna/intent/api/v1/network-
        device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
            'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```

Cisco DNA Center APIのこのPythonスクリプトの結果は何ですか？

- A. スイッチに関する情報を受信します
- B. スイッチに認証を追加します
- C. CiscoDNACenterにスイッチを追加します

正解: ([正解を表示します](#))

質問: 312

管理者は、ネットワークで使用されているアプリケーションを特定しようとしています。ネットワークデバイスがCiscoFirepowerにメタデータを送信することを望んでいません。これを実現するには、どの機能を使用する必要がありますか？

- A. パケットトレーサー
- B. NetFlow
- C. ネットワークディスカバリー
- D. アクセス制御

正解: **C** ([コメントを發表する](#))

質問: 313

エンジニアは、ネットワーク上のトラフィックの中断に気づきます。さらに調査すると、ブロードキャストパケットがネットワークにフラッディングしていることがわかりました。この問題に対処するには、事前定義されたしきい値に基づいて何を構成する必要がありますか？

- A. Bridge Protocol Data Unit Guard
- B. 組み込みイベントの監視
- C. ストームコントロール
- D. アクセス制御リスト

正解: ([正解を表示します](#))

説明

説明

ストーム制御は、LAN上のトラフィックが、物理インターフェイスの1つでのブロードキャスト、マルチキャスト、またはユニキャストストームによって中断されるのを防ぎます。パケットがLANにフラッディングすると、LANストームが発生し、過剰なトラフィックが発生し、ネットワークパフォーマンスが低下します。プロトコルスタックの実装におけるエラー、ネットワーク構成の誤り、またはサービス拒否攻撃を発行するユーザーは、ストームを引き起こす可能性があります。

ストーム制御ブロードキャストレベル[立ち下がりしきい値]」を使用することにより、スイッチのブロードキャストトラフィックを制限できます。

質問: 314

ネットワーク管理者は、ネットワーク上に現在存在する資産を確認する必要があります。サードパーティシステムは、ホストデータをCiscoFirepowerにフィードできる必要があります。これを達成するために最も構成されているものは何ですか？

- A. ホストからデータを受信するためのネットワーク検出ポリシー
- B. ホストからNetFlowデータを受信するためのネットワーク分析ポリシー
- C. ファイルデータをCiscoFirepowerに送信するためのファイル分析ポリシー
- D. ホストからデータをダウンロードするための脅威インテリジェンスポリシー

正解: **A** ([コメントを發表する](#))

質問: 315

テナントが仮想マシンOSのパッチ適用を担当するクラウドサービスモデルはどれですか？

- A. PaaS
- B. IaaS
- C. SaaS
- D. UCaaS

正解: ([正解を表示します](#))

質問: 316

DNSトンネリングは、企業ネットワークからデータを盗み出すためにどのように使用されますか？

- A. 再帰的なルックアップを許可してDNSサーバーを活用し、攻撃を他のDNSサーバーに拡散します。
- B. 短い文字列に分割されたランダムな文字でペイロードをエンコードし、DNSサーバーが抽出されたデータを再構築します。
- C. DNS要求を、ユーザーの資格情報を盗むために使用される悪意のあるサーバーにリダイレクトします。これにより、ネットワークがさらに損傷したり盗まれたりする可能性があります。
- D. 実際のIPアドレスを不正なアドレスに置き換えて情報を収集したり、他の攻撃を開始したりすることで、DNSサーバーを破壊します。

正解: ([正解を表示します](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 317

エンジニアは、デバイス管理のためのTACACS+認証および許可のためのソリューションを必要としています。エンジニアはまた、ユーザーとエンドポイントに使用を要求することにより、有線および無線ネットワークのセキュリティを強化したいと考えています。

802.1X、MAB、またはWebAuth。これらの要件をすべて満たす製品はどれですか？

- A. CiscoPrimeインフラストラクチャ
- B. Cisco Identity Services Engine
- C. エンドポイント向けCisco AMP
- D. Cisco Stealthwatch

正解: ([正解を表示します](#))

質問: 318

エンドポイントに最新のOSアップデートとパッチがシステムにインストールされているかどうかを判断するシスコのセキュリティソリューションはどれですか。

- A. エンドポイントコンプライアンススキャナー
- B. セキュリティ姿勢評価サービス
- C. Cisco Endpoint Security Analytics
- D. エンドポイント向けCisco AMP

正解: B ([コメントを發表する](#))

質問: 319

CiscoASAプラットフォームで有効なRESTAPIの2つの要求方法はどれですか。(2つ選択してください。)

- A. 置く
- B. オプション
- C. 取得

D. プッシュ

E. 接続

正解: (正解を表示します)

説明/リファレンス <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

質問: 320

セキュリティイベントのみをログに記録するようにCiscoUmbrellaを構成するにはどうすればよいですか。

A. ポリシーごと

B. レポート設定で

C. [セキュリティ設定]セクション

D. [展開]セクションのネットワークごと

正解: A (コメントを發表する)

説明/参照 <https://docs.umbrella.com/deployment-umbrella/docs/log-management>

質問: 321

ネットワークリソースにアクセスするために、証明書を展開し、モバイルデバイスにサプリカントを構成するために使用される方法はどれですか。

A. 搭乗中のBYOD

B. 単純な証明書登録プロトコル

C. クライアントプロビジョニング

D. MAC認証バイパス

正解: A (コメントを發表する)

企業ネットワークで個人用デバイスをサポートする場合は、ユーザー（従業員 請負業者、ゲスト）とそのデバイスを認証および承認することにより、ネットワークサービスと企業データを保護する必要があります。Cisco ISEは、従業員が企業ネットワーク上でパーソナルデバイスを安全に使用できるようにするために必要なツールを提供します。ゲストは、ネイティブサプリカントプロビジョニング（ネットワークセットアップアシスタント）を実行するか、デバイスをマイデバイスポータルに追加することにより、個人のデバイスをネットワークに追加できます。ネイティブサプリカントプロファイルはすべてのデバイスで利用できるわけではないため、ユーザーはマイデバイスポータルを使用してこれらのデバイスを手動で追加できます。または、Bring Your Own Device（BYOD）ルールを構成して、これらのデバイスを登録することもできます。参照：

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod ユーザー（従業員 請負業者、ゲスト）とそのデバイスを認証および承認することによるhtmlデータ。Cisco ISEは、従業員が企業ネットワーク上でパーソナルデバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ネイティブサプリカントプロビジョニング（ネットワークセットアップアシスタント）を実行するか、デバイスをマイデバイスポータルに追加することにより、個人のデバイスをネットワークに追加できます。

ネイティブサプリカントプロファイルはすべてのデバイスで利用できるわけではないため、ユーザーはマイデバイスポータルを使用してこれらのデバイスを手動で追加できます。または、Bring Your Own Device（BYOD）ルールを構成して、これらのデバイスを登録することもできます。

参照：

企業ネットワークで個人用デバイスをサポートする場合は、ユーザー（従業員 請負業者、ゲスト）とそのデバイスを認証および承認することにより、ネットワークサービスと企業データを保護する必要があります。Cisco ISEは、従業員が企業ネットワーク上でパーソナルデバイスを安全に使用できるようにするために必要なツールを提供します。ゲストは、ネイティブサプリカントプロビジョニング（ネットワークセットアップアシスタント）を実行するか、デバイスをマイデバイスポータルに追加することにより、個人のデバイスをネットワークに追加できます。ネイティブサプリカントプロファイルはすべてのデバイスで利用できるわけではないため、ユーザーはマイデバイスポータルを使用してこれらのデバイスを手動で追加できます。また

は、Bring Your Own Device (BYOD)ルールを構成して、これらのデバイスを登録することもできます。参照：
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html

質問: 322

Cisco AMPforEndpointsをネットワークにインストールする利点は何ですか。

- A. セキュリティのためにエンドポイントにオペレーティングシステムのパッチを提供します。
- B. エンドポイントのネットワーク接続にフローベースの可視性を提供します。
- C. アプリケーション制御とリアルタイムスキャンを通じてエンドポイントシステムを保護します。
- D. エンドポイントに動作分析を使用できるようにします。

正解: C ([コメントを发表する](#))

説明

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance>

質問: 323

展示を参照してください。

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept' : application/json
    'content-type' : application/json
    'authorization' : Basic API Credentials
    'cache-control' : "no-cache"
}
response = requests.request ("GET", url, headers = headers)
print (response.txt)
```

このPythonスクリプトを実行するとどうなりますか？

- A. 侵害されたコンピュータとマルウェアの軌跡はCiscoAMPから受信されます
- B. コンピュータとその現在の脆弱性のリストはCiscoAMPから受信されます
- C. 侵害されたコンピュータとそれらを侵害したものはCiscoAMPから受信されます
- D. コンピュータ、ポリシー、およびコネクタのステータスのリストがCiscoAMPから受信されます

正解: D ([コメントを发表する](#))

`https://api.amp.cisco.com/v1/computers`のAPIを呼び出すと、Advanced Malware Protection (AMP)が参照している組織全体のコンピューターのリストを取得できます `https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1` Advanced Malware Protection (AMP)が参照する組織参照：

`https://api.amp.cisco.com/v1/computers`のAPIを呼び出すと、Advanced Malware Protection (AMP)が参照している組織全体のコンピューターのリストを取得できます `https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1`

質問: 324

最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

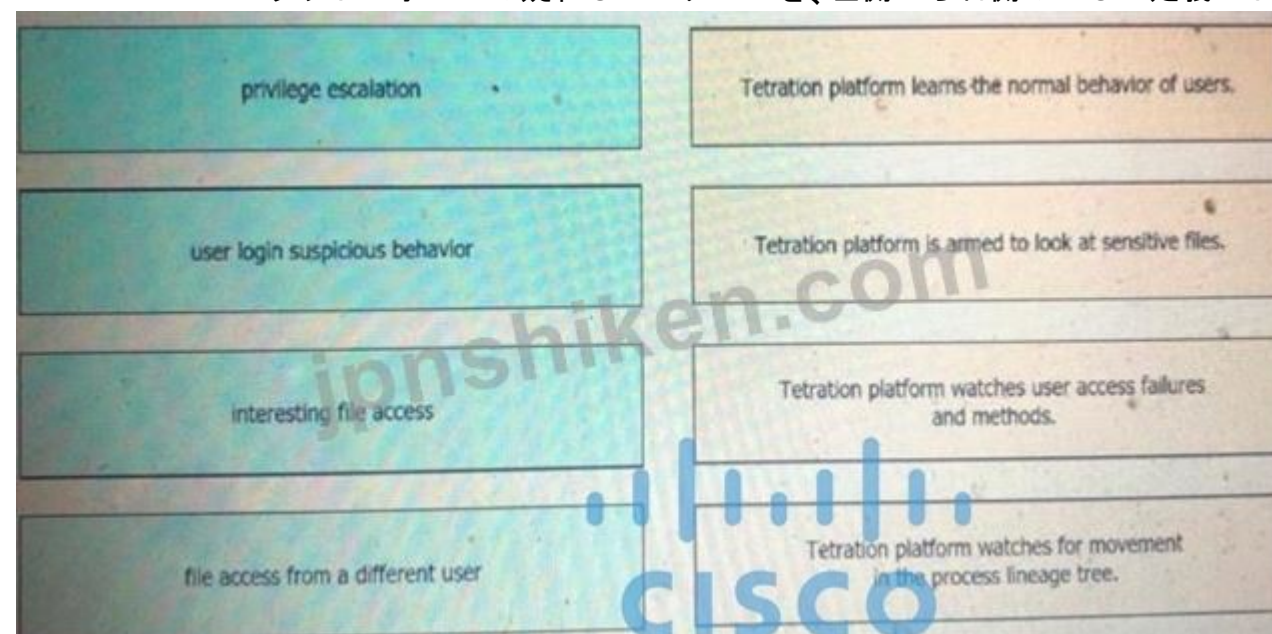
- A. アクセスポリシーを変更します。
- B. 識別プロファイルを変更します。
- C. アウトバウンドマルウェアスキャンポリシーを変更する
- D. Webプロキシ設定を変更する

正解: (正解を表示します)

An explicit proxy deployment is when a client **proxy-aware application**, like a mature web browser, has a configuration area within for proxy settings to declare and use a proxy, like the WSA. This method is typically combined with a firewall restricting web traffic that does not originate from the WSA's IP to prevent users from circumventing web policy controls and accessing

質問: 325

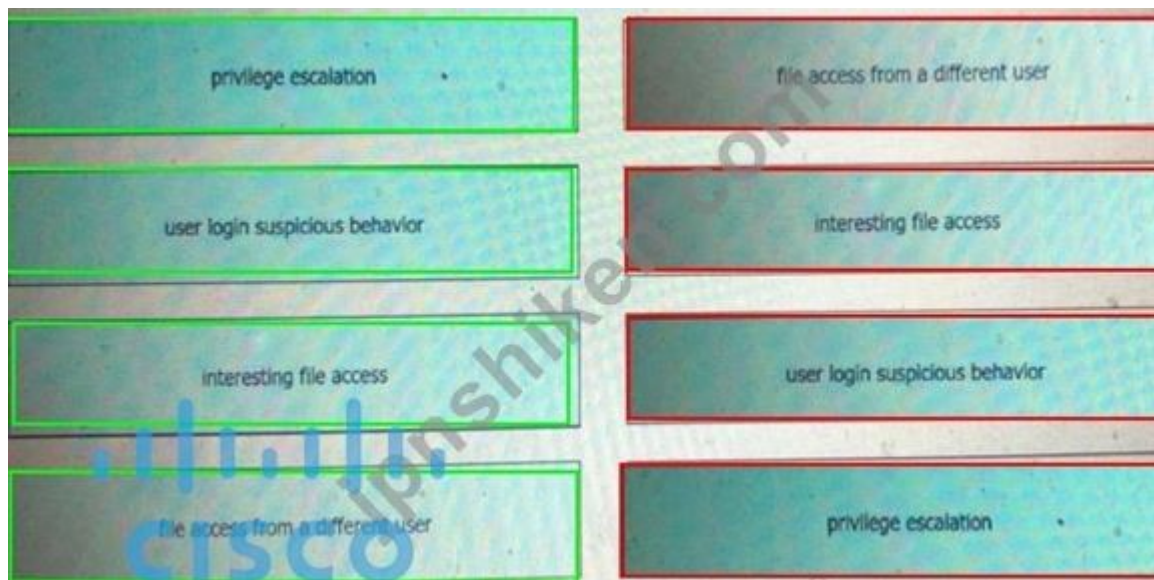
Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。



The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:

- **Shell code execution:** Looks for the patterns used by shell code.
- **Privilege escalation:** Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
- **Side channel attacks:** Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these
- **Raw socket creation:** Creation of a raw socket by a nonstandard process (for example, ping).
- **User login suspicious behavior:** Cisco Tetration platform watches user login failures and user login methods.
- **Interesting file access:** Cisco Tetration platform can be armed to look at sensitive files.
- **File access from a different user:** Cisco Tetration platform learns the normal behavior of which file is accessed by which
- **Unseen command:** Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command. lineage triggers the interest of the Tetration Analytics platform. (See Figure 10.)

正解:



<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html>

質問: 326

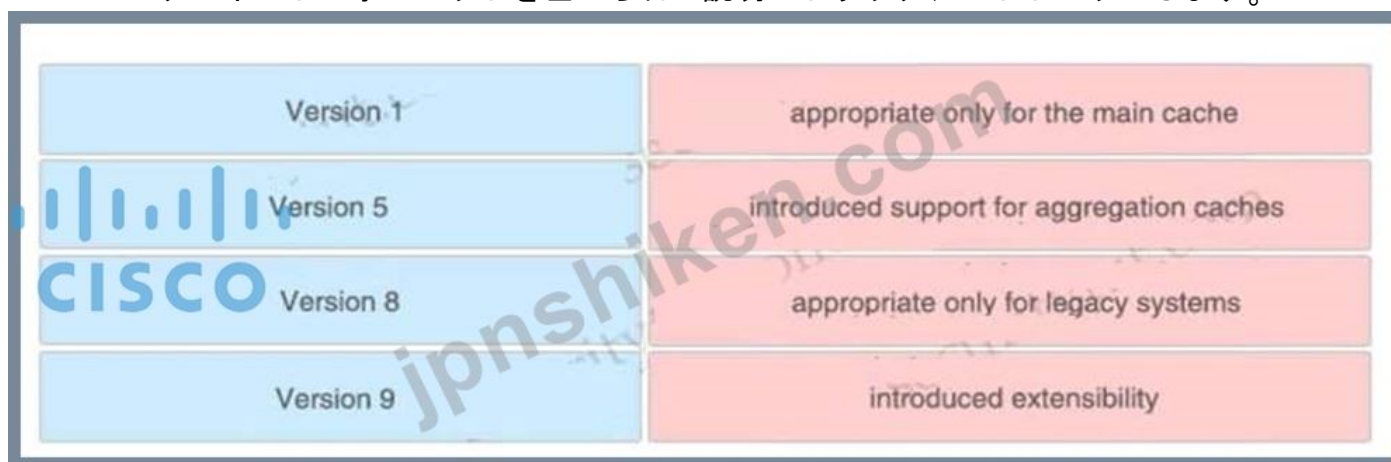
Cisco Umbrellaは、クライアントが企業ネットワークの外部で動作している場合、どのようにクライアントを保護しますか？

- A. 企業のネームサーバーにDNSクエリを強制する
- B. CiscoUmbrellaローミングクライアントを使用する
- C. DNSルックアップのレジストリを変更する
- D. ActiveDirectoryグループポリシーを使用してCiscoUmbrellaDNSサーバを適用する

正解: ([正解を表示します](#))

質問: 327

NetFlowエクスポートフォーマットを左から右の説明にドラッグアンドドロップします。



正解:



質問: 328

メッセージングプロトコルの2つの特性のうち、データの漏えいを検出および防止するのが難しいのはどれですか？
2つ選択してください)

- A. マルウェアは、ユーザーエンドポイントのメッセージングアプリケーションに感染して、会社のデータを送信します。
- B. ユーザーが外部組織と通信できるように、送信トラフィックが許可されます。
- C. メッセージングプラットフォーム用の公開されたAPIは、大量のデータを送信するために使用されます。
- D. メッセージングアプリケーションを標準のネットワークコントロールでセグメント化することはできません
- E. トラフィックは暗号化されているため、ファイアウォールやIPSシステムでの可視性が妨げられます。

正解: ([正解を表示します](#))

質問: 329

Cisco Advanced Phishing Protectionはどのようにユーザーを保護しますか？

- A. DKIMを使用して送信者を検証します。
- B. 送信者がどのIDを認識するかを決定します
- C. メッセージを安全に送信するセンサーを利用しています。
- D. 機械学習とリアルタイムの行動分析を使用します。

正解: ([正解を表示します](#))

Cisco Advanced Phishing Protectionは、送信者認証およびBEC検出機能を提供します。高度な機械学習技術、リアルタイムの行動分析、関係モデリング、およびテレメトリを使用して、ID詐欺に基づく脅威から保護します。参照 <https://docs.ces.cisco.com/docs/advanced-phishing-protection> Cisco Advanced Phishing Protectionは、送信者認証およびBEC検出機能を提供します。高度な機械学習技術、リアルタイムの行動分析、関係モデリング、およびテレメトリを使用して、ID詐欺に基づく脅威から保護します。参照 <https://docs.ces.cisco.com/docs/advanced-phishing-protection>

質問: 330

コグニティブ脅威分析の2つの検出および分析エンジンとは何ですか？ 2つ選択してください。)

- A. インテリジェントプロキシ
- B. URLの分類
- C. snort
- D. データの漏えい
- E. コマンドアンドコントロール通信

正解: ([正解を表示します](#))

質問: 331

Firepower Next Generation Intrusion Prevention System検出器を、左側から右側の正しい定義にドラッグアンドドロップします。

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

正解:

PortScan Detection

Port Sweep

Decoy PortScan

Distributed PortScan

Distributed PortScan

Decoy PortScan

Port Sweep

PortScan Detection

Distributed PortScan

Decoy PortScan

Port Sweep

PortScan Detection

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 332

ネットワークエンジニアがsnmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941コマンドを入力し、SNMP情報を10.255.254.1のホストに送信する必要があります。この目標を達成するコマンドはどれですか？

- A. 10.255.254.1バージョン3andy内のsnmp-serverホスト
- B. 10.255.254.1バージョン3myv3内のsnmp-serverホスト
- C. 10.255.254.1 snmpv3andy内のsnmp-serverホスト
- D. 10.255.254.1 snmpv3myv3内のsnmp-serverホスト

正解: ([正解を表示します](#))

コマンド "snmp-server user user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]"は、新しいユーザー（この場合は"andy"）をSNMPv3グループ（この場合はグループ名"myv3"）に追加し、ユーザーのパスワードを構成します。

「snmp-server host」コマンドでは、次のことを行う必要があります。

+キーワード「version {1 | 2 | 3}」でSNMPバージョンを指定します

+グループ名（"myv3"）ではなく、ユーザー名（"andy"）を指定します。

注：「snmp-server host inside ...」コマンドで、「inside」は、NMS（10.255.254.1にある）に到達できるASAインターフェイスのインターフェイス名です。

質問: 333

IPsecのステートフルフェールオーバーの前提条件となる2つの条件はどれですか。2つ選択してください

- A. アクティブデバイスに設定されているIKE構成のみを、スタンバイデバイスに複製する必要があります。IPsec構成が自動的にコピーされます
- B. アクティブデバイスとスタンバイデバイスは、異なるバージョンのCisco IOSソフトウェアを実行できますが、同じタイプのデバイスである必要があります。
- C. アクティブデバイスで設定されているIPsec構成は、スタンバイデバイスで複製する必要があります
- D. アクティブデバイスで設定されているIPsec構成のみを、スタンバイデバイスで複製する必要があります。IKE構成は自動的にコピーされます。
- E. アクティブデバイスとスタンバイデバイスは、同じバージョンのCisco IOSソフトウェアを実行し、同じタイプのデバイスである必要があります

正解: ([正解を表示します](#))

説明

IPセキュリティ（IPsec）のステートフルフェールオーバーにより、計画的または計画外の停止が発生した後も、ルータはIPsecパケットの処理と転送を続行できます。お客様は、アクティブルータが何らかの理由で接続を失った場合に、アクティブ（プライマリ）ルータのタスクを自動的に引き継ぐバックアップ（セカンダリ）ルータを採用しています。このフェイルオーバープロセスはユーザーに対して透過的であり、リモートピアの調整や再構成は必要ありません。

IPsecのステートフルフェールオーバーでは、ネットワークに、プライマリデバイスまたはセカンダリデバイスとして使用できる2つの同一のルータが含まれている必要があります。両方のルータは同じタイプのデバイスであり、同じCPUとメモリを備え、暗号化アクセラレータがないか、同じ暗号化アクセラレータを備えている必要があります。

IPsecのステートフルフェールオーバーの前提条件

アクティブデバイスとスタンバイデバイスでの完全な重複IPsecおよびIKE構成このドキュメントは、完全なIKEおよびIPsec構成があることを前提としています。アクティブデバイスで設定されているIKEおよびIPsec設定は、スタンバイデバイスで複製する必要があります。つまり、暗号構成は、インターネットセキュリティアソシエーションおよびキー管理プロトコル（ISAKMP）ポリシー、ISAKMPキー（事前共有）、IPsecプロファイル、IPsecトランスフォームセット、ステートフルフェールオーバーに使用されるすべての暗号マップセット、すべてのアクセスに関して同一である必要があります。クリプトマップセットのマッチアドレスステートメントで使用するコントロールリスト（ACL）、クリプトに使用されるすべてのAAA設定、クライアントコンフィギュレーショングループ、クリプトに使用されるIPローカルプール、およびISAKMPプロファイル。参照 <https://www.cisco.com>。

このドキュメントは、完全なIKEおよびIPsec構成があることを前提としています。

アクティブデバイスで設定されているIKEおよびIPsec設定は、スタンバイデバイスで複製する必要があります。

つまり、暗号構成は、インターネットセキュリティアソシエーションおよびキー管理プロトコル (ISAKMP) ポリシー、ISAKMPキー (事前共有) IPsec プロファイル、IPsec トランスフォームセット、ステートフルフェールオーバーに使用されるすべての暗号マップセット、すべてのアクセスに関して同一である必要があります。クリプトマップセットのマッチアドレスステートメントで使用されるコントロールリスト (ACL)、クリプトに使用されるすべてのAAA設定、クライアントコンフィギュレーショングループ、クリプトに使用されるIPローカルプール、およびISAKMPプロファイル。

参照：

前提条件は 両方のルーターは同じタイプのデバイスである必要がある」とだけ述べていますが、アクティブデバイスとスタンバイデバイスでの完全な

重複IPsecおよびIKE構成このドキュメントは、完全なIKEおよびIPsec構成があることを前提としています。アクティブデバイスで設定されているIKEおよびIPsec設定は、スタンバイデバイスで複製する必要があります。つまり、暗号構成は、インターネットセキュリティアソシエーションおよびキー管理プロトコル (ISAKMP) ポリシー、ISAKMPキー (事前共有) IPsec プロファイル、IPsec トランスフォームセット、ステートフルフェールオーバーに使用されるすべての暗号マップセット、すべてのアクセスに関して同一である必要があります。クリプトマップセットのマッチアドレスステートメントで使用されるコントロールリスト (ACL)、クリプトに使用されるすべてのAAA設定、クライアントコンフィギュレーショングループ、クリプトに使用されるIPローカルプール、およびISAKMPプロファイル。参照 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnv/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.html前提条件では、両方のルータは同じタイプのデバイスである必要があります」とだけ記載されていますが、上記のリンクの「IPsecのステートフルフェールオーバーの制限」セクションでは、「アクティブデバイスとスタンバイデバイスの両方を実行する必要があります」が必要です。同一バージョンのCisco IOS ソフトウェア」であるため、回答Eは回答Bよりも優れています。

質問: 334

組織はクラウド環境でデータを保護したいそのセキュリティモデルでは、すべてのユーザーを認証および承認する必要がありますアプリケーションとデータへのアクセスを許可または維持する前に、セキュリティ構成とポスチャを継続的に検証する必要があります特定のアプリケーショントラフィックを許可する必要もありますデフォルトで他のすべてのトラフィックを拒否するこれらの要件を実装するには、どのテクノロジーを使用する必要がありますか？

- A. 仮想ルーティングと転送
- B. アクセス制御ポリシー
- C. 仮想LAN
- D. マイクロセグメンテーション

正解: B ([コメントを发表する](#))

質問: 335

多要素認証で最も一般的に使用される2つの認証要素は何ですか？ 2つ選択してください。)

- A. 暗号化係数
- B. 知識要素
- C. 生体認証係数
- D. 時間係数
- E. 守秘義務

正解: ([正解を表示します](#))

質問: 336

Cisco IOS PKIの場合、CRLの配布ポイントとして使用される2種類のサーバはどれですか。2つ選択してください)

- A. SDP
- B. LDAP
- C. 下位CA
- D. SCP
- E. HTTP

正解: ([正解を表示します](#))

Cisco IOS公開鍵基盤 (PKI)は、IPセキュリティ (IPSec)、セキュアシェル (SSH)、セキュアソケットレイヤ (SSL)などのセキュリティプロトコルをサポートする証明書管理を提供します。このモジュールでは、PKIを理解、計画、および実装するために必要な概念を特定して説明します。

PKIは、次のエンティティで構成されています。

-証明書失効リスト (CRL)の配布メカニズム ライトウェイトディレクトリアクセスプロトコル[LDAP]やHTTPなど) Cisco IOS公開鍵基盤 (PKI)は、IPセキュリティ (IPSec)、セキュアシェル (セキュアシェル)などのセキュリティプロトコルをサポートする証明書管理を提供します。SSH)、およびセキュアソケットレイヤー (SSL)。このモジュールでは、PKIを理解、計画、および実装するために必要な概念を特定して説明します。

PKIは、次のエンティティで構成されています。

-証明書失効リスト (CRL)の配布メカニズム ライトウェイトディレクトリアクセスプロトコル[LDAP]やHTTPなど) リファレンス :

Cisco IOS公開鍵基盤 (PKI)は、IPセキュリティ (IPSec)、セキュアシェル (SSH)、セキュアソケットレイヤ (SSL)などのセキュリティプロトコルをサポートする証明書管理を提供します。このモジュールでは、PKIを理解、計画、および実装するために必要な概念を特定して説明します。

PKIは、次のエンティティで構成されています。

-証明書失効リスト (CRL)の配布メカニズム ライトウェイトディレクトリアクセスプロトコル[LDAP]やHTTPなど)

質問: 337

エンジニアは、ネットワーク上のトラフィックの中断に気づきます。さらに調査すると、ブロードキャストパケットがネットワークにフラッディングしていることがわかりました。この問題に対処するには、事前定義されたしきい値に基づいて何を構成する必要がありますか？

- A. Bridge Protocol Data Unit Guard
- B. 組み込みイベントの監視
- C. アクセス制御リスト
- D. ストームコントロール

正解: ([正解を表示します](#))

説明

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e1.html>

質問: 338

マネージドインテークラウドファブリックデプロイメントモデルの2つのタイプは何ですか？ 2つ選択してください。)

- A. パブリックマネージド
- B. サービスプロバイダーが管理
- C. ユーザー管理
- D. エンタープライズ管理
- E. ハイブリッドマネージド

正解: ([正解を表示します](#))

質問: 339

ネットワークエンジニアがDMVPNを設定しており、ホストAでcrypto isakmp key cisc0380739941address0.0.0.0コマンドを入力しました。ホストBへのトンネルが確立されていません。

VPNを認証するにはどのようなアクションが必要ですか？

- A. ホストAのコマンドでisakmpをikev2に変更します。
- B. ホストAのパスワードをデフォルトのパスワードに変更します。
- C. ホストBで同じコマンドを入力します。
- D. ホストBで別のパスワードを使用してコマンドを入力します。

正解: [\(正解を表示します\)](#)

質問: 340

組織は複数のCiscoFTDアプライアンスを導入しており、1つの集中型ソリューションを使用してそれらを管理したいと考えています。組織にはローカルVMはありませんが、CiscoFTDに移行する必要がある既存のCiscoASAがあります。組織のニーズを満たすソリューションはどれですか？

- A. Cisco FMC
- B. CSM
- C. CDO
- D. Cisco FDM

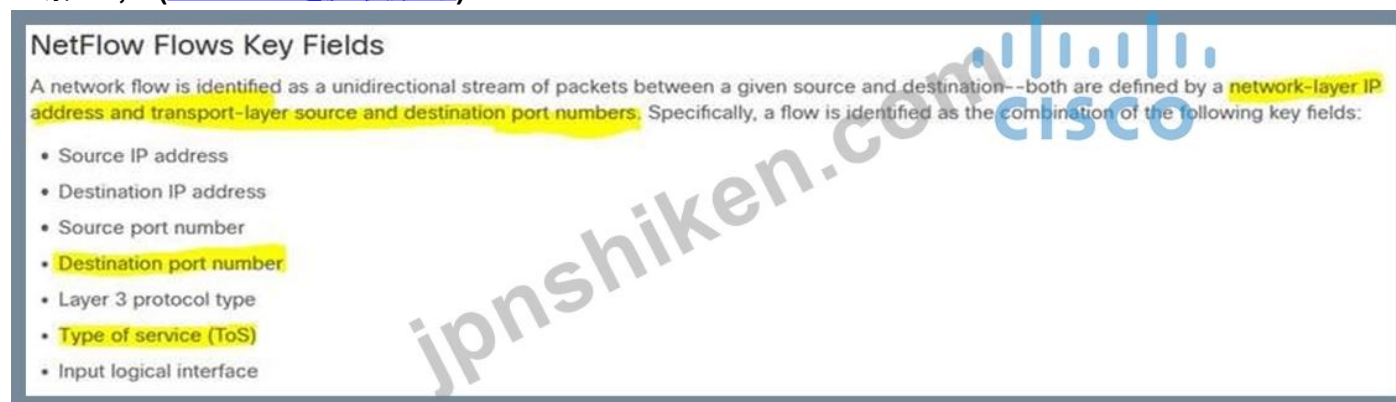
正解: **A** ([コメントを発表する](#))

質問: 341

NetFlowフローで定義されている2つのフィールドはどれですか？{2つ選択してください。}

- A. サービスバイトのタイプ
- B. レイヤー4プロトコルタイプ
- C. サービスクラスビット
- D. 出力論理インターフェース
- E. 宛先ポート

正解: **A,E** ([コメントを発表する](#))



The diagram titled "NetFlow Flows Key Fields" explains that a network flow is a unidirectional stream of packets between a source and destination, both defined by a network-layer IP address and transport-layer source and destination port numbers. It lists the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

質問: 342

Cisco ESAネットワーク管理者は、新しくインストールされたサービスを使用して、レピュテーション判定に基づいたポリシーの作成を支援するように任命されています。テスト中に、CiscoESAが未決定の評決を持つファイルをドロップしていないことがわかりました。この問題の原因は何ですか？

- A. ポリシーは、ドロップではなく隔離にメッセージを送信するために作成されました

- B. ファイルのレピュテーションスコアがしきい値を超えています
- C. ファイルのレピュテーションスコアがしきい値を下回っています
- D. ファイル分析を無効にするポリシーが作成されました

正解: D (コメントを发表する)

この質問の「新しくインストールされたサービス」は、ESAと一緒に使用できるAdvanced Malware Protection (AMP)について言及している可能性があります。AMPは、攻撃の連続体全体で優れた保護を可能にします。

+ファイルレピュテーション-ESAを通過するときに各ファイルのフィンガープリントをキャプチャし、レピュテーション判定のためにAMPのクラウドベースのインテリジェンスネットワークに送信します。これらの結果があれば、悪意のあるファイルを自動的にブロックし、管理者が定義したポリシーを適用できます。

+ファイル分析-ESAを通過している未知のファイル进行分析する機能を提供します。高度に安全なサンドボックス環境により、AMPはファイルの動作に関する正確な詳細を収集し、そのデータを詳細な人間およびマシンの分析と組み合わせて、ファイルの脅威レベルを判断できます。次に、この処理はAMPクラウドベースのインテリジェンスネットワークに送られ、AMPクラウドデータセットを動的に更新および拡張して保護を強化するために使用されます。

質問: 343

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

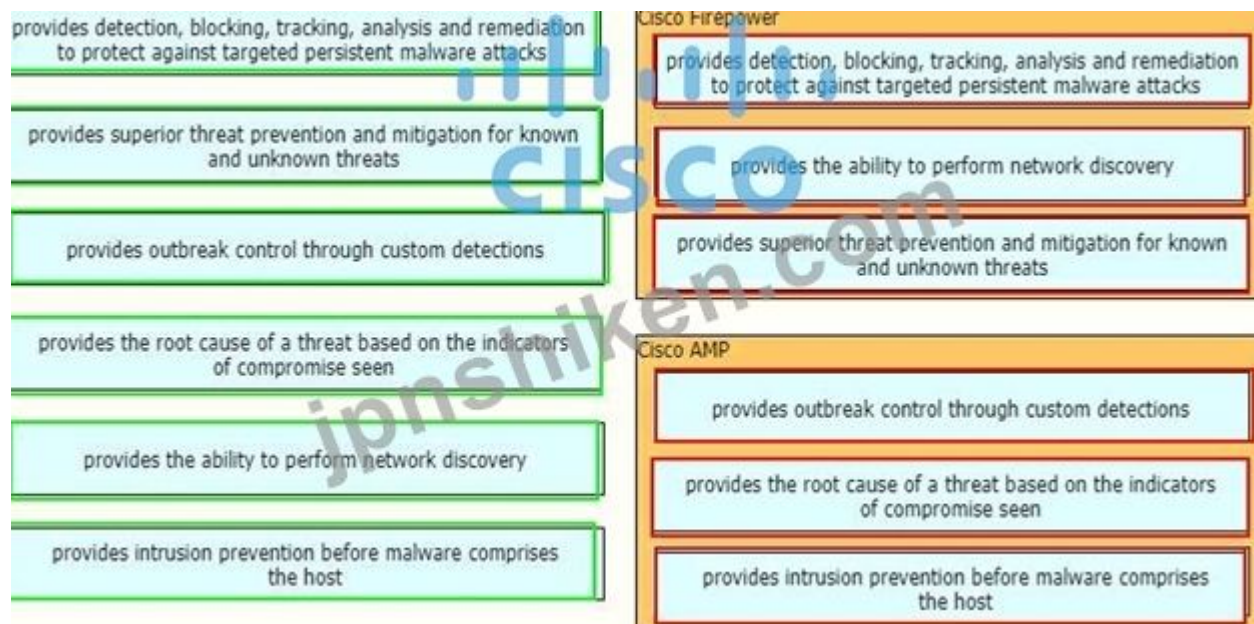
provides the ability to perform network discovery

provides intrusion prevention before malware compromises the host

Cisco Firepower

Cisco AMP

正解:



質問: 344

VPN機能を左から右の説明にドラッグアンドドロップします。



正解:



質問: 345

エンジニアは、Cisco Umbrella SecureInternetGatewayを使用してネットワークのWebフィルタリングを設定しています。

要件は、すべてのトラフィックをフィルタリングする必要があることです。SSL復号化機能を使用して、この目標を達成するためにエンドユーザーに提示する必要がある証明書のタイプはどれですか。

- A. SubCA
- B. サードパーティ
- C. 組織所有のルート
- D. 自己署名

正解: ([正解を表示します](#))

質問: 346

Cisco DNA Centerの2つの機能のうち、ソフトウェア定義ネットワークソリューションで使用されているものはどれですか。2つ選択してください

- A. 会計
- B. 保証
- C. 自動化
- D. 認証
- E. 暗号化

正解: B,C ([コメントを發表する](#))

Cisco DNA Centerで自動化できる機能：単一のダッシュボードを使用してネットワークを管理および自動化することにより、時間を節約します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。安全なポリシー：ビジネスニーズに基づいて、グループベースの安全なアクセスとネットワークセグメンテーションを展開します。Cisco DNA Centerを使用すると、ネットワークデバイスではなく、ユーザとアプリケーションにポリシーを適用できます。自動化により、手動操作と人的エラーに関連するコストが削減され、稼働時間の増加とセキュリティの向上が実現します。次に、Assuranceはネットワークを評価し、コンテキストを使用してデータをインテリジェンスに変換し、ネットワークデバイスポリシーの変更が意図を達成していることを確認します。保証：監視識別、ネットワークとワイヤレスの状態の変化にリアルタイムで対応します。Cisco DNA Centerは、ネットワークの有線および無線デバイスを使用してあらゆる場所にセンサーを作成し、実際のネットワーク状態に基づいてリアルタイムのフィードバックを提供します。Cisco DNA Assuranceエンジンは、ネットワークセンサーの洞察をストリーミングテレメトリと関連付け、これをこれらのデータソースの現在のコンテキストと比較します。Cisco DNA Centerダッシュボードでヘルススコアをすばやく確認すると、パフォーマンスの問題がある場所を確認し、最も可能性の高い原因を数分で特定できます。エコシステムの拡張：新しいCisco DNA Centerプラットフォームにより、ITはCiscoソリューションとサードパーティテクノロジーを単一のネットワークオペレーションに統合して、ITワークフローを合理化し、ビジネス価値とイノベーションを向上させることができます。Cisco DNA Centerを使用すると、ITおよびビジネスアプリケーションとのオープンインターフェイスでネットワークを実行し、IT運用およびテクノロジードメイン間で統合し、異種ネットワークデバイスを管理できます。参照 <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html> Automate：単一のダッシュボードを使用してネットワークを管理および自動化することにより、時間を節約します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。[com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html) 自動化：単一のダッシュボードを使用して管理することで時間を節約しますネットワークを自動化します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。[com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html) 自動化：単一のダッシュボードを使用して管理することで時間を節約しますネットワークを自動化します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。

安全なポリシー：ビジネスニーズに基づいて、グループベースの安全なアクセスとネットワークセグメンテーションを展開します。Cisco DNA Centerを使用すると、ネットワークデバイスではなく、ユーザとアプリケーションにポリシーを適用できます。自動化により、手動操作と人的エラーに関連する

コストが削減され、稼働時間の増加とセキュリティの向上が実現します。次に、Assuranceはネットワークを評価し、コンテキストを使用してデータをインテリジェンスに変換し、ネットワークデバイスポリシーの変更が意図を達成していることを確認します。

保証 : ネットワークとワイヤレスの状態の変化をリアルタイムで監視、識別、対応します。Cisco DNA Centerは、ネットワークの有線および無線デバイスを使用してあらゆる場所にセンサーを作成し、実際のネットワーク状態に基づいてリアルタイムのフィードバックを提供します。Cisco DNA Assuranceエンジンは、ネットワークセンサーの洞察をストリーミングテレメトリと関連付け、これをこれらのデータソースの現在のコンテキストと比較します。Cisco DNA Centerダッシュボードでヘルススコアをすばやく確認すると、パフォーマンスの問題がある場所を確認し、最も可能性の高い原因を数分で特定できます。

エコシステムの拡張 : 新しいCisco DNA Centerプラットフォームにより、ITはCiscoソリューションとサードパーティテクノロジーを単一のネットワークオペレーションに統合して、ITワークフローを合理化し、ビジネス価値とイノベーションを向上させることができます。Cisco DNA Centerを使用すると、ITおよびビジネスアプリケーションとのオープンインターフェイスでネットワークを実行し、IT運用およびテクノロジードメイン間で統合し、異種ネットワークデバイスを管理できます。

Cisco DNA Centerで自動化できる機能 : 単一のダッシュボードを使用してネットワークを管理および自動化することにより、時間を節約します。直感的なワークフローと再利用可能なテンプレートを使用して、ビジネスを迅速に拡張します。企業全体で数千のネットワークデバイスを数時間ではなく数分で構成およびプロビジョニングします。安全なポリシー : ビジネスニーズに基づいて、グループベースの安全なアクセスとネットワークセグメンテーションを展開します。Cisco DNA Centerを使用すると、ネットワークデバイスではなく、ユーザとアプリケーションにポリシーを適用できます。自動化により、手動操作と人的エラーに関連するコストが削減され、稼働時間の増加とセキュリティの向上が実現します。次に、Assuranceはネットワークを

評価し、コンテキストを使用してデータをインテリジェンスに変換し、ネットワークデバイスポリシーの変更が意図を達成していることを確認します。保証 : 監視 識別、ネットワークとワイヤレスの状態の変化にリアルタイムで対応します。Cisco DNA Centerは、ネットワークの有線および無線デバイスを使用してあらゆる場所にセンサーを作成し、実際のネットワーク状態に基づいてリアルタイムのフィードバックを提供します。Cisco DNA Assuranceエンジンは、ネットワークセンサーの洞察をストリーミングテレメトリと関連付け、これをこれらのデータソースの現在のコンテキストと比較します。Cisco DNA Centerダッシュボードでヘルススコアをすばやく確認すると、パフォーマンスの問題がある場所を確認し、最も可能性の高い原因を数分で特定できます。エコシステムの拡張 : 新しいCisco DNA Centerプラットフォームにより、ITはCiscoソリューションとサードパーティテクノロジーを単一のネットワークオペレーションに統合して、ITワークフローを合理化し、ビジネス価値とイノベーションを向上させることができます。Cisco DNA Centerを使用すると、ITおよびビジネスアプリケーションとのオープンインターフェイスでネットワークを実行し、IT運用およびテクノロジードメイン間で統合し、異種ネットワークデバイスを管理できます。参照 <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-cisco-dna-center-aag-cte-en.html>

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **347**

展示を参照してください。

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                  = AUTHENTICATOR
PortControl          = FORCE_AUTHORIZED
ControlDirection     Both
HostMode             = SINGLE_HOST
QuietPeriod          = 60
ServerTimeout        = 0
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30
```

この出力を表示するために使用されたコマンドはどれですか？

- A. dot1xのすべての概要を表示
- B. dot1xallを表示
- C. dot1xを表示
- D. show dot1x interface gi1 / 0/12

正解: [\(正解を表示します\)](#)

質問: 348

説明を左側から右側の暗号化アルゴリズムにドラッグアンドドロップします。

requires secret keys

requires more time

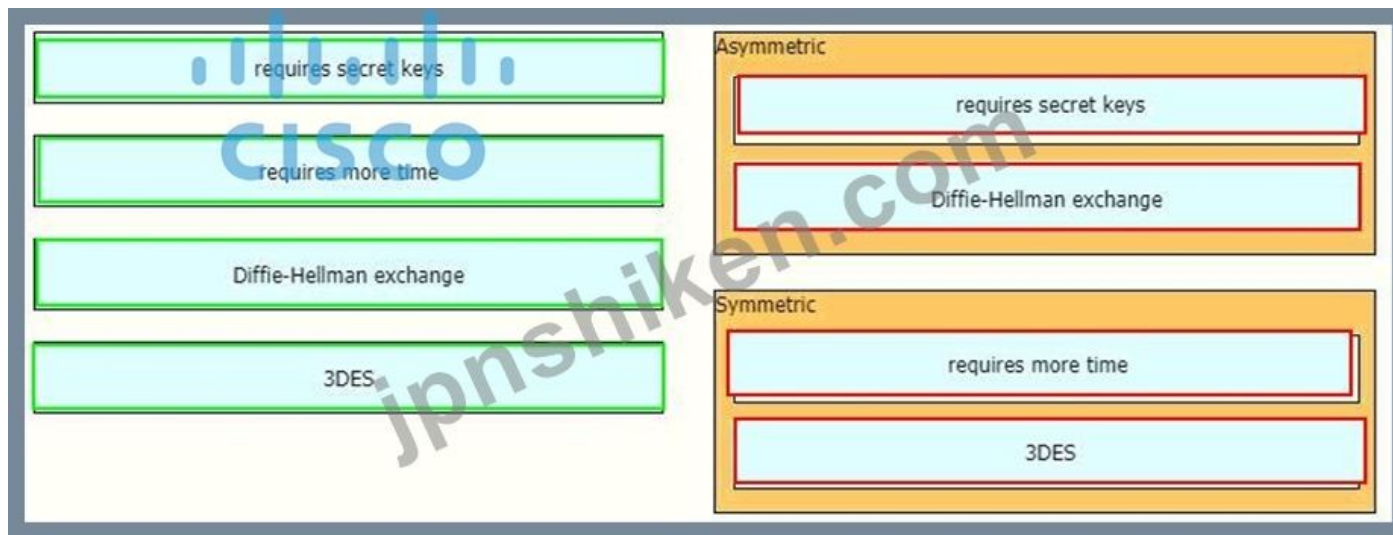
Diffie-Hellman exchange

3DES

Asymmetric

Symmetric

正解:



質問: 349

クラウドPaaSモデルのどの2つの側面が顧客によって管理されていますが、プロバイダーによっては管理されていませんか？ 2つ選択してください。）

- A. 仮想化
- B. ミドルウェア
- C. オペレーティングシステム
- D. アプリケーション
- E. データ

正解: ([正解を表示します](#))

参照 :

<https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/>

質問: 350

どの姿勢評価要件がクライアントに修復のオプションを提供し、特定の時間枠内の修復を必要としますか？

- A. オーディオ
- B. 必須
- C. 可視性
- D. オプション

正解: A ([コメントを发表する](#))

質問: 351

DuoSecurityが組織に提供するような多要素認証ソリューションを実装する2つの理由は何ですか？ 2つ選択してください）

- A. 電話のコールバック、SMSパスコード、プッシュ通知など、2FAのさまざまな方法の柔軟性
- B. オンプレミスおよびクラウドアプリケーションへのシングルサインオンアクセス
- C. ネイティブのMicrosoft Windows サプリカントを使用した802.1xセキュリティとの統合
- D. オンプレミスおよびクラウドアプリケーションへの安全なアクセス
- E. リソースへのアクセスを許可する前のアプリケーションの脆弱性の特定と修正

正解: ([正解を表示します](#))

説明

二要素認証は、オンラインアカウントにセキュリティの第2層を追加します。2番目の要素（電話やその他のモバイルデバイスなど）を使用して本人確認を行うと、パスワードを知っている場合でも、自分以外の人にはログインできなくなります。

注 :シングルサインオン (SSO)は、IDおよびアクセス管理のプロパティであり、ユーザーは1セットの資格情報（ユーザー名とパスワード）で1回だけログインすることにより、複数のアプリケーションとWebサイトで安全に認証できます。SSOを使用すると、ユーザーがアクセスしようとしているアプリケーションまたはWebサイトは、信頼できるサードパーティに依存して、ユーザーが本人であることを確認します。

質問: 352

ネットワーク管理者は、アクセス制御ポリシーで特定のURLをブロックするルールを構成し、「チャットとインスタントメッセージング」カテゴリを選択しています。この目標を達成するには、どのレピュテーションスコアを選択する必要がありますか？

- A. 1
- B. 10
- C. 5
- D. 3

正解: ([正解を表示します](#))

https://www.cisco.com/c/en/us/td/docs/security/esa/esa111/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01111.html

質問: 353

組織は、DNSサービスに使用されるようにCiscoUmbrellaを設定します。組織は、エンドポイントが存在するサブネットに基づいてトラフィックをブロックできる必要がありますが、各内部IPアドレスではなく、パブリックIPアドレスからの要求のみが表示されます。この問題を解決するには何をする必要がありますか？

- A. Cisco Umbrella仮想アプライアンスをセットアップして、要求を内部的に処理し、各IPアドレスのトラフィックを確認します
- B. Cisco Umbrella内に内部ドメインを設定して、各アドレスを識別し、ドメインからポリシーを作成できるようにします
- C. テナント制御機能を使用して、使用されている各サブネットを識別し、CiscoUmbrellaダッシュボード内の接続を追跡します
- D. Microsoft Active Directoryコネクタをインストールして、CiscoUmbrellaダッシュボードの要求に関連付けられたIPアドレス情報を提供します

正解: ([正解を表示します](#))

質問: 354

展示を参照してください。

The screenshot shows the 'Add Device' configuration window for a Cisco FTD device. The 'Registration Key' field is highlighted with a red box and contains the text 'Unique, user-defined key used to register device'. Other fields include Host (1.1.1.2), Display Name (FTD123), Group (FTD_Group), Access Control Policy (FTD Policy), and Smart Licensing options (Malware, Threat, URL Filtering, Advanced, Unique NAT ID, Transfer Packets). The Cisco logo is visible in the background.

管理者が新しいCiscoFTDデバイスをネットワークに追加していて、CiscoFMCで管理したいと考えています。

CiscoFTDはNATデバイスの背後にありません。Cisco FTDでこれを有効にするには、どのコマンドが必要ですか。

- A. マネージャーを構成してDONTRESOLVE登録キーを追加>
- B. configure manager add <FMC IP address> <registration key> 16
- C. configure manager addDONTRESOLVE<登録キー>FTD123
- D. configure manager add <FMC IP address> <registration key>

正解: D (コメントを发表する)

Explanation:説明 :FMCにFTDを管理させるには、まずFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド configuremanageradd 1.1.1.2 the_registration_key_you_want 1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。参照 https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/説明 :

FMCにFTDを管理させるには、まずFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド configuremanageradd 1.1.1.2 the_registration_key_you_want 1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。

Explanation:説明 :FMCにFTDを管理させるには、まずFTDからマネージャーを追加し、選択したレジスタキーを割り当てる必要があります。コマンド configuremanageradd 1.1.1.2 the_registration_key_you_want 1.1.1.2はFMCのIPアドレス)。このFTDを管理対象デバイスとして追加する場合は、FMCで同じ登録キーを使用する必要があります。参照 https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/

質問: 355

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

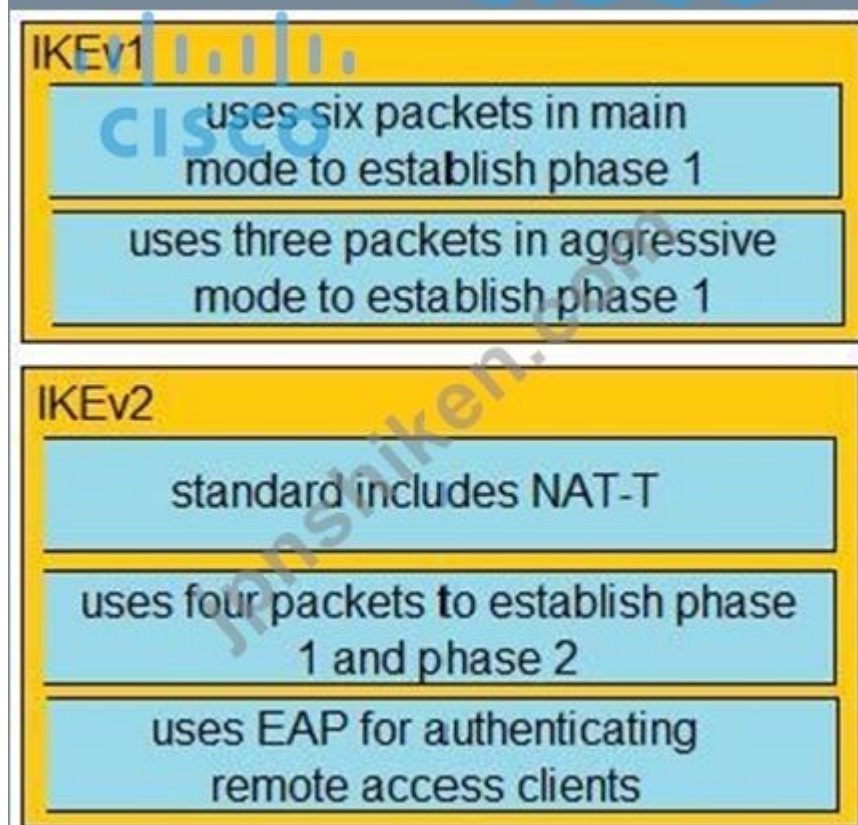
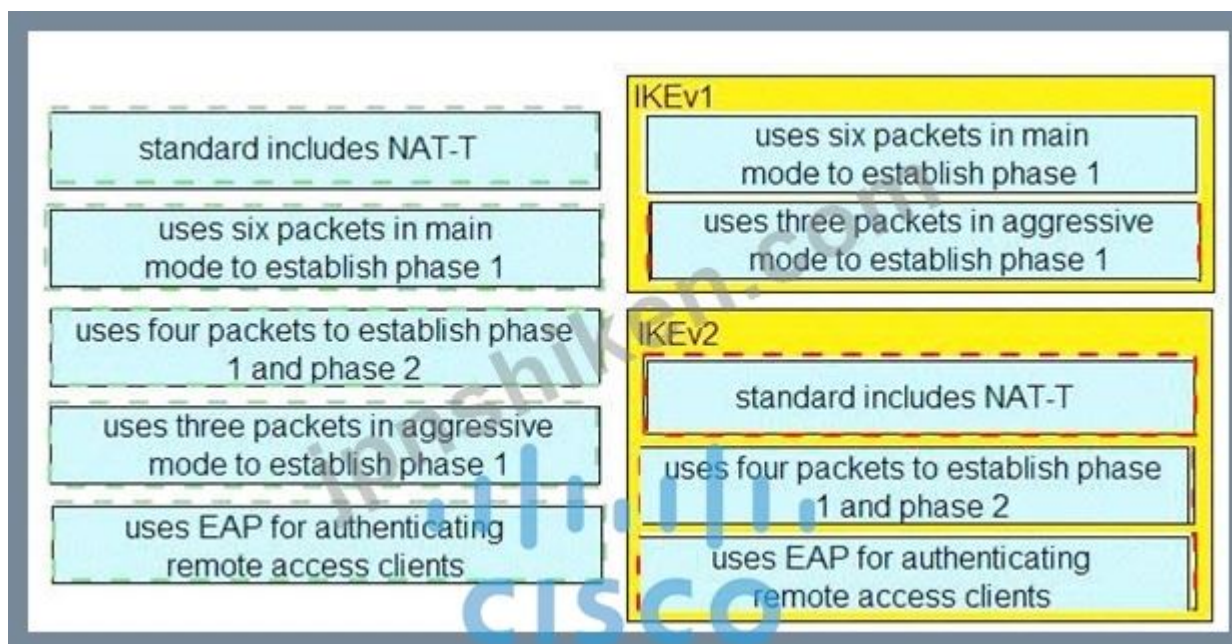
uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

正解:



質問: 356

展示を参照してください。

```
snmp-server group SNMP v3 auth access
15
```

この構成では、15という数字は何を表していますか？

- A. このルーターに対する許可されたユーザーの特権レベル
- B. ルーターにアクセスできるSNMPデバイスを識別するアクセスリスト
- C. SNMPv3認証の試行間の秒単位の間隔
- D. SNMPv3ユーザーがロックアウトされるまでに失敗した可能性のある試行の数

正解: ([正解を表示します](#))

このコマンドの構文を以下に示します。

snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]]] [read read-view] [write write-view] [notify notify-view] [access access-list]上記のコマンドは、ルータのSNMP機能へのアクセスを許可するIP送信元アドレスを制限します。インターフェイスACLを適用するだけで、SNMPアクセスを制限して、信頼できるサーバーから送信されない着信SNMPパケットをブロックできます。ただし、これは、このレシピに示されているグローバルSNMPコマンドを使用する場合ほど効果的ではありません。この方法はルータ全体に1回適用できるため、ACLを適用してすべてのインターフェイスでSNMPを個別にブロックするよりもはるかに簡単です。また、インターフェイスACLを使用すると、このルーター向けのSNMPパケットがブロックされるだけでなく、他の宛先デバイスに向かう途中でたまたま通過したSNMPパケットが停止する可能性があります。

質問: 357

IPsecのステートフルフェールオーバーの前提条件となる2つの条件はどれですか。 2つ選択してください。）

- A. アクティブデバイスで設定されているIPsec構成のみを、スタンバイデバイスで複製する必要があります。IKE構成は自動的にコピーされます
- B. アクティブデバイスとスタンバイデバイスは、同じバージョンのCisco IOSソフトウェアを実行し、同じタイプのデバイスである必要があります
- C. アクティブデバイスに設定されているIKE構成のみを、スタンバイデバイスに複製する必要があります。IPsec構成が自動的にコピーされます。
- D. アクティブデバイスとスタンバイデバイスは、異なるバージョンのCisco IOSソフトウェアを実行できますが、同じタイプのデバイスである必要があります。
- E. アクティブデバイスで設定されているIPsec構成は、スタンバイデバイスで複製する必要があります。

正解: ([正解を表示します](#))

質問: 358

任意から任意のスケラブルな接続を備えたプライベートIPクラウドを介して会社の支店間で安全なVPN接続を実装するには、どのテクノロジーを使用する必要がありますか？

- A. DMVPN
- B. FlexVPN
- C. IPsec DVTI
- D. VPNを取得

正解: ([正解を表示します](#))

説明シスコのグループ暗号化トランスポートVPN (GETVPN)は、ポイントツーポイントトンネルとそれに関連するオーバーレイルーティングを排除するためのトラステッドグループの概念を導入しています。すべてのグループメンバー (GM)は、グループSAとも呼ばれる共通のセキュリティアソシエーション (SA)を共有します。これにより、GMは他のGMによって暗号化されたトラフィックを復号化できます。GETVPNは、グループIPsecセキュリティパラダイムを使用して、瞬時に大規模なany-to-anyIP接続を提供します。参照 https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_2_0_External.pdf

質問: 359

Cisco ESAネットワーク管理者は、新しくインストールされたサービスを使用して、レピュテーション判定に基づいたポリシーの作成を支援するように任命されています。テスト中に、CiscoESAが未確定の判定を持つファイルをドロップしていないことが判明しました。この問題の原因は何ですか。

- A. ファイルのレピュテーションスコアがしきい値を超えています
- B. ポリシーは、ドロップではなく隔離にメッセージを送信するために作成されました
- C. ファイル分析を無効にするポリシーが作成されました
- D. ファイルのレピュテーションスコアがしきい値を下回っています

正解: C ([コメントを发表する](#))

質問: 360

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

superior threat prevention and mitigation
for known and unknown threats

detection, blocking, tracking, analysis,
and remediation to protect against
targeted persistent malware attacks

application-layer control and ability to
enforce usage and tailor detection policies
based on custom applications and URLs

combined integrated solution of strong
defense and web protection, visibility, and
controlling solutions

質問: 361

802.1 x展開でMAB要求をフィルタリングするために使用できるRADIUS属性はどれですか？

- A. 1
- B. 2
- C. 6
- D. 31

正解: (正解を表示します)

MABはMACアドレスをユーザー名とパスワードとして使用するため、RADIUSサーバーがMAB要求を他の種類のネットワークアクセス要求と区別できることを確認する必要があります。この予防措置により、他のクライアントがMACアドレスを有効な資格情報として使用しようとするのを防ぐことができます。Ciscoスイッチは、MAB Access-Requestメッセージで属性6 (Service-Type)を10 (Call-Check)に設定することにより、MAB要求を一意に識別します。したがって、属性6を使用して、RADIUSサーバーでMAB要求をフィルタリングできます。参照 https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html属性6 サービス-MAB Access-Requestメッセージに)から10 (Call-Check)を入力します。したがって、属性6を使用して、RADIUSサーバーでMAB要求をフィルタリングできます。

MABはMACアドレスをユーザー名とパスワードとして使用するため、RADIUSサーバーがMAB要求を他の種類のネットワークアクセス要求と区別できることを確認する必要があります。この予防措置により、他のクライアントがMACアドレスを有効な資格情報として使用しようとするのを防ぐことができます。Ciscoスイッチは、MAB Access-Requestメッセージで属性6 (Service-Type)を10 (Call-Check)に設定することにより、MAB要求を一意に識別します。したがって、属性6を使用して、RADIUSサーバーでMAB要求をフィルタリングできます。参照 https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **362**

エンジニアは、トラフィックを監視し、イベントに基づいてインシデントを作成し、APIを介して他のクラウドソリューションと統合するクラウドソリューションを必要としています。この目標を達成するには、どのソリューションを使用する必要がありますか？

A. SIEM

B. CASB

C. アダプティブMFA

D. Cisco Cloudlock

正解: ([正解を表示します](#))

+ Cisco Cloudlockは、クラウドデータ損失防止 (DLP) エンジンを使用してクラウド環境を継続的に監視し、ポリシーに違反してクラウド環境に保存されている機密情報を特定します。

+CloudlockはAPIベースです。

+インシデントは、CiscoCloudlockアプリケーションの重要なリソースです。これらは、ポリシー検出基準によってオブジェクト (ドキュメント、フィールド、フォルダー、投稿、またはファイル) が一致したときに、Cloudlockポリシーエンジンによってトリガーされます。

+ Cisco Cloudlockは、クラウドデータ損失防止 (DLP) エンジンを使用してクラウド環境を継続的に監視し、ポリシーに違反してクラウド環境に保存されている機密情報を特定します。

+CloudlockはAPIベースです。

+インシデントは、CiscoCloudlockアプリケーションの重要なリソースです。これらは、ポリシー検出基準によってオブジェクト (ドキュメント、フィールド、フォルダー、投稿、またはファイル) が一致したときに、Cloudlockポリシーエンジンによってトリガーされます。

参照：

ノート：

+セキュリティ情報およびイベント管理 (SIEM) プラットフォームは、セキュリティシステム、ネットワーク、およびコンピューターからログおよびイベントデータを収集し、それを実用的なセキュリティインサイトに変換します。

+インシデントは、アラートポリシーのトリガーの記録です。Cloud Monitoringは、アラートポリシーの条件が満たされたときにインシデントを開きます。

+ Cisco Cloudlockは、クラウドデータ損失防止 (DLP) エンジンを使用してクラウド環境を継続的に監視し、ポリシーに違反してクラウド環境に保存されている機密情報を特定します。

+CloudlockはAPIベースです。

+インシデントは、CiscoCloudlockアプリケーションの重要なリソースです。これらは、ポリシー検出基準によってオブジェクト (ドキュメント、フィールド、フォルダー、投稿、またはファイル) が一致したときに、Cloudlockポリシーエンジンによってトリガーされます。

ノート：

+セキュリティ情報およびイベント管理 (SIEM) プラットフォームは、セキュリティシステム、ネットワーク、およびコンピューターからログおよびイベントデータを収集し、それを実用的なセキュリティインサイトに変換します。

+インシデントは、アラートポリシーのトリガーの記録です。注 :Cloud Monitoringは、次の場合にインシデントを開きます。

+セキュリティ情報およびイベント管理 (SIEM) プラットフォームは、セキュリティシステム、ネットワーク、およびコンピューターからログおよびイベントデータを収集し、それを実用的なセキュリティインサイトに変換します。

+インシデントは、アラートポリシーのトリガーの記録です。Cloud Monitoringは、アラートポリシーの条件が満たされたときにインシデントを開きます。

質問: **363**

16進表現などの代替エンコーディングが最も頻繁に観察される攻撃の形式はどれですか？

- A. スマーフ
- B. 分散型サービス拒否
- C. クロスサイトスクリプティング
- D. ルートキットエクспロイト

正解: **C** ([コメントを发表する](#))

説明

クロスサイトスクリプティング (XSSとも呼ばれます)は、Webアプリケーションがユーザーから悪意のあるデータを収集するときに発生します。データは通常、悪意のあるコンテンツを含むハイパーリンクの形式で収集されます。ユーザーは、別のWebサイト、インスタントメッセージ、または単にWebボードや電子メールメッセージを読んでいるときに、このリンクをクリックする可能性があります。

通常、攻撃者はサイトへのリンクの悪意のある部分をHEX または他のエンコード方法)でエンコードするため、クリックされたときに要求がユーザーに見えることはそれほど疑わしくありません。

たとえば、以下のコードは16進数で記述されています。<a

href = javascript :alert & #

x28'XSS')>ここをクリック

と同等です :

ここをクリック

注 : & #xhhhh」の形式では、hhhhは16進形式のコードポイントです。

質問: **364**

エンドポイント保護プラットフォームではなく、エンドポイント検出および応答ソリューションを選択する必要があるのはどのような状況ですか？

- A. 従来のマルウェア対策検出が必要な場合
- B. ソリューションを一元管理する必要がない場合
- C. ネットワーク上にファイアウォールがない場合
- D. より高度な検出機能が必要な場合

正解: ([正解を表示します](#))

説明

説明

エンドポイント保護プラットフォーム (EPP)は、既知および未知のマルウェアなどのエンドポイントセキュリティの脅威を防ぎます。

エンドポイント検出および応答 (EDR)ソリューションは、EPPやその他のセキュリティツールが検出できなかった脅威を検出して応答できます。

EDRとEPPの目標は似ていますが、異なる目的を達成するように設計されています。EPPは、悪意のあるファイルを識別し、潜在的に悪意のあるアクティビティを検出し、インシデントの調査と対応のためのツールを提供することにより、デバイスレベルの保護を提供するように設計されています。

EPPの予防的性質は、予防的EDRを補完します。EPPは防御の最前線として機能し、組織の展開されたセキュリティソリューションによって検出される可能性のある攻撃を除外します。EDRは、保護の第2層として機能し、セキュリティアナリストが脅威ハンティングを実行し、エンドポイントに対するより微妙な脅威を特定できるようにします。

効果的なエンドポイント防御には、EDRとEPPの両方の機能を統合して、組織のセキュリティチームを圧倒することなくサイバー脅威に対する保護を提供するソリューションが必要です。

質問: **365**

ストリームを使用して運用データをプッシュし、アクティビティのほぼリアルタイムのビューを提供するネットワーク監視ソリューションはどれですか？

- A. モデル駆動型テレメトリ
- B. syslog
- C. SMTP
- D. SNMP

正解: ([正解を表示します](#))

質問: **366**

CiscoESAでは防止できるがCiscoWSAでは防止できない攻撃はどれですか。

- A. バッファオーバーフロー
- B. DoS
- C. SQLインジェクション
- D. フィッシング

正解: ([正解を表示します](#))

Cisco EmailSecurityGatewayにCiscoAdvancedPhishingProtectionを導入する利点は次のとおりです。
次のことを防ぎます。

- +侵害されたアカウントとソーシャルエンジニアリングを使用する攻撃。
- +フィッシング、ランサムウェア、ゼロデイ攻撃、なりすまし。
- +悪意のあるペイロードまたはURLのないBEC。

Cisco EmailSecurityGatewayにCiscoAdvancedPhishingProtectionを導入する利点は次のとおりです。
次のことを防ぎます。

- +侵害されたアカウントとソーシャルエンジニアリングを使用する攻撃。
- +フィッシング、ランサムウェア、ゼロデイ攻撃、なりすまし。
- +悪意のあるペイロードまたはURLのないBEC。

Cisco EmailSecurityGatewayにCiscoAdvancedPhishingProtectionを導入する利点は次のとおりです。
次のことを防ぎます。

- +侵害されたアカウントとソーシャルエンジニアリングを使用する攻撃。
- +フィッシング、ランサムウェア、ゼロデイ攻撃、なりすまし。
- +悪意のあるペイロードまたはURLのないBEC。

参照：

5 / m_advanced_phishing_protection.html

5 / m_advanced_phishing_protection.html

質問: **367**

クラウドアクセスセキュリティブローカーはどのように機能しますか？

- A. ネットワーク内で使用されている他のクラウドソリューションをスキャンし、脆弱性を特定します
- B. APIを介して他のクラウドソリューションと統合し、クラウドソリューションからのイベントに基づいてインシデントを監視および作成します
- C. クラウドソリューションのシングルサインオンおよび多要素認証を有効にする認証ブローカーです
- D. セキュリティ情報およびイベント管理ソリューションとして機能し、他のクラウドソリューションからsyslogを受信します。

正解: ([正解を表示します](#))

質問: **368**

Cisco DNA Centerのオーブンプラットフォーム機能の機能は何ですか？

- A. アプリケーションアダプタ
- B. ドメイン統合
- C. 自動化アダプター
- D. インテントベースのAPI

正解: ([正解を表示します](#))

質問: **369**

TAXIIプロトコルを介して転送できる脅威インテリジェンスを交換するために設計された言語フォーマットとは何ですか？

- A. XMPP
- B. STIX
- C. SMTP
- D. pxGrid

正解: ([正解を表示します](#))

質問: **370**

VPNのセキュアハッシュアルゴリズムによって何が提供されますか？

- A. 整合性
- B. 鍵交換
- C. 暗号化
- D. 認証

正解: ([正解を表示します](#))

HMAC-SHA-1-96 (HMAC-SHA-1とも呼ばれます) 暗号化技術は、メッセージが変更されていないことを確認するためにIPSecによって使用されます。(>したがって、 整合性」と答えるのが最良の選択です)。HMAC-SHA-1は、FIPS-190-1で指定されたSHA-1をHMACと組み合わせて使用し RFC 2104に準拠)、RFC2404で説明されています。

HMAC-SHA-1-96 (HMAC-SHA-1とも呼ばれます) 暗号化技術は、メッセージが変更されていないことを確認するためにIPSecによって使用されます。(>したがって、 整合性」と答えるのが最良の選択です)。HMAC-SHA-1は、FIPS-190-1で指定されたSHA-1をHMACと組み合わせて使用し RFC 2104に準拠)、RFC2404で説明されています。

参照：

HMAC-SHA-1-96 (HMAC-SHA-1とも呼ばれます) 暗号化技術は、メッセージが変更されていないことを確認するためにIPSecによって使用されます。(>したがって、 整合性」と答えるのが最良の選択です)。HMAC-SHA-1は、FIPS-190-1で指定されたSHA-1をHMACと組み合わせて使用し RFC 2104に準拠)、RFC2404で説明されています。

質問: 371

DMVPNとsVTIの違いは何ですか？

- A. DMVPNは他のベンダーとの相互運用性を提供しますが、sVTIは提供しません。
- B. DMVPNはトンネル暗号化をサポートしていますが、sVTIはサポートしていません。
- C. DMVPNは動的トンネル確立をサポートしますが、sVTIはサポートしません。
- D. DMVPNは静的トンネルの確立をサポートしますが、sVTIはサポートしません。

正解: ([正解を表示します](#))

質問: 372

エンジニアがMicrosoftWindowsエンドポイントでポスチャチェックを使用し、MS17-010パッチがインストールされていないことを発見しました。これにより、エンドポイントがWannaCryランサムウェアに対して脆弱なままになりました。このランサムウェア感染のリスクを軽減する2つのソリューションはどれですか？ 2つ選択してください)

- A. ネットワークへのアクセスを許可する前にMS17-010パッチをインストールするようにCisco IdentityServicesEngineでポスチャポリシーを設定します。
- B. ネットワークへのアクセスを許可する前にパッチレベルを確認してエンドポイントを設定するように、Cisco IdentityServiceEngineでプロファイリングポリシーを設定します。
- C. ネットワークでのアクセスを許可する前にエンドポイントパッチレベルが満たされていることを確認するために、Cisco IdentityServicesEngineでポスチャポリシーを設定します。
- D. エンドポイントファイアウォールポリシーを構成して、エクスプロイトトラフィックがネットワーク全体で実行および複製されないようにします。
- E. 明確に定義されたエンドポイントのパッチ適用戦略を設定して、エンドポイントに重大な脆弱性にタイムリーにパッチが適用されるようにします。

正解: ([正解を表示します](#))

説明

ポスチャポリシーは、1つ以上のIDグループとオペレーティングシステムに関連付けられているポスチャ要件のコレクションです。[ワークセンター]>[ポスチャ]>[ポスチャ要素]>[条件]>[ファイル]でWindowsパッチをチェックするようにISEを設定できます。

この例では、事前定義されたファイルチェックを使用して、WannaCryマルウェアを防ぐためにWindows10クライアントに重要なセキュリティパッチがインストールされていることを確認します。

File Conditions List > [pc_W10_64_KB4012606_Ms17-010_1507_W](#)

File Condition

* Name **pc_W10_64_KB4012606_Ms1**

Description **Cisco Predefined Check: Micro**

* Operating System **Windows 10 (All)**

Compliance Module **Any version**

* File Type **FileVersion**

* File Path **SYSTEM_32**

* Operator **LaterThan**

* File Version **10.0.10240.17318**

Cancel

質問: 373

展示を参照してください。

```
aaa new-model
```

```
radius-server host 10.0.0.12 key secret12
```

構成で使用する認証プロトコルに関する説明のうち正しいものはどれですか。

- A. 認証要求にはパスワードのみが含まれています
- B. 認証要求パケットと承認要求パケットが別々にあります。
- C. 認証および承認要求は1つのパケットにグループ化されます。
- D. 認証要求にはユーザー名のみが含まれます

正解: ([正解を表示します](#))

質問: 374

SDNサウスバウンドAPIプロトコルの機能は何ですか？

- A. コントローラーが変更を行えるようにする
- B. コントロールプレーンアプリケーションの動的構成を可能にするため
- C. コントローラーがRESTを使用できるようにします
- D. コントロールプレーンアプリケーションの静的構成を可能にするため

正解: ([正解を表示します](#))

参照 :

Southbound APIs facilitate control over the network and enable the **SDN Controller** to dynamically make changes according to real-time demands and needs.

質問: 375

Cisco Advanced Phishing Protectionはどのようにユーザーを保護しますか？

- A. DKIMを使用して送信者を検証します。
- B. 送信者がどのIDを認識するかを決定します
- C. メッセージを安全に送信するセンサーを利用しています。
- D. 機械学習とリアルタイムの行動分析を使用します。

正解: D ([コメントを发表する](#))

Cisco Advanced Phishing Protectionは、送信者認証およびBEC検出機能を提供します。高度な機械学習技術、リアルタイムの行動分析、関係モデリング、およびテレメトリを使用して、ID詐欺に基づく脅威から保護します。

Cisco Advanced Phishing Protectionは、送信者認証およびBEC検出機能を提供します。高度な機械学習技術、リアルタイムの行動分析、関係モデリング、およびテレメトリを使用して、ID詐欺に基づく脅威から保護します。

参照：

Cisco Advanced Phishing Protectionは、送信者認証およびBEC検出機能を提供します。高度な機械学習技術、リアルタイムの行動分析、関係モデリング、およびテレメトリを使用して、ID詐欺に基づく脅威から保護します。

質問: 376

組織は、短期間に大量のスパムメッセージを受信しました。メッセージに対してアクションを実行するには、メッセージがどれほど有害であるかを判断する必要があります、これは動的に発生する必要があります。

これを実現するには何を構成する必要がありますか？

- A. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoWSAを設定します。
- B. Talosからリアルタイムアップデートを受信するようにCiscoESAを設定します
- C. Talosからリアルタイムアップデートを受信するようにCiscoWSAを設定します。
- D. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoESAを設定します。

正解: B ([コメントを发表する](#))

説明

https://www.cisco.com/c/en/us/td/docs/security/esa/esa120/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Adm

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 377

Cisco IOS PKIの場合、CRLの配布ポイントとして使用される2種類のサーバはどれですか。(2つ選択してください)

- A. SDP
- B. LDAP

- C. 下位CA
- D. SCP
- E. HTTP

正解: ([正解を表示します](#))

説明Cisco IOS公開鍵基盤 (PKI)は、IPセキュリティ (IPSec)、セキュアシェル (SSH)、セキュアソケットレイヤ (SSL)などのセキュリティプロトコルをサポートする証明書管理を提供します。このモジュールでは、PKIを理解、計画、および実装するために必要な概念を特定して説明します。PKIは、次のエンティティで構成されています。...-証明書失効リスト (CRL)の配布メカニズム (Lightweight Directory Access Protocol [LDAP]やHTTPなど) 参照 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html説明 Cisco IOS公開鍵インフラストラクチャ (PKI)は、IPセキュリティ (IPSec)、セキュアシェル (SSH)、セキュアソケットレイヤー (SSL)などのセキュリティプロトコルをサポートします。

PKIは、次のエンティティで構成されています。

-証明書失効リスト (CRL)の配布メカニズム ライトウェイトディレクトリアクセスプロトコル[LDAP]やHTTPなど) 説明Cisco IOS公開鍵インフラストラクチャ (PKI)は、IPセキュリティ (IPSec)などのセキュリティプロトコルをサポートする証明書管理を提供します。シェル (SSH)、およびセキュアソケットレイヤー (SSL)。このモジュールでは、PKIを理解、計画、および実装するために必要な概念を特定して説明します。PKIは、次のエンティティで構成されています。...-証明書失効リスト (CRL)の配布メカニズム ライトウェイトディレクトリアクセスプロトコル[LDAP]やHTTPなど) 参照 :

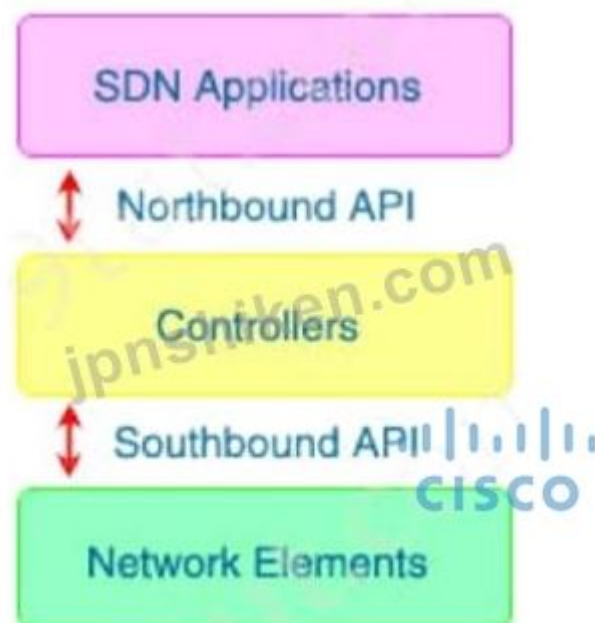
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html

質問: 378

ソフトウェア定義ネットワークアーキテクチャ内のサウスバウンドAPIはどのコンポーネントと通信しますか？

- A. ネットワーク内のコントローラー
- B. アプリケーション
- C. アプライアンス
- D. ルーターやスイッチなどのデバイス

正解: ([正解を表示します](#))



サウスバウンドAPIは、コントローラーとネットワークデバイス間の通信に使用されます。

質問: 379

多要素認証で最も一般的に使用される2つの認証要素は何ですか？ 2つ選択してください。)

- A. 暗号化係数
- B. 時間係数
- C. 生体認証係数
- D. 守秘義務
- E. 知識要素

正解: C,E ([コメントを發表する](#))

質問: 380

DNAC GUI以外の場所からネットワークをプログラムおよび監視する機能を提供するものは何ですか？

- A. NetFlow
- B. ASDM
- C. デスクトップクライアント
- D. API

正解: ([正解を表示します](#))

質問: 381

エンドポイントがIDグループから削除されたときに、エンドポイントセッションの再認証を強制するには、Cisco ISEで何を設定する必要がありますか。

- A. 姿勢評価
- B. CoA
- C. 外部IDソース
- D. SNMPプローブ

正解: ([正解を表示します](#))

Cisco ISEでは、グローバルコンフィギュレーションで[ProfilerConfiguration]ページで[Changeof Authorization CoA)]を発行できます。これにより、プロファイリングサービスは、すでに認証されているエンドポイントをより詳細に制御できます。

CoAタイプを構成するための設定の1つは、再認証」です。このオプションは、プロファイリング時に、すでに認証されているエンドポイントの再認証を強制するために使用されます。

Cisco ISEでは、グローバルコンフィギュレーションで[ProfilerConfiguration]ページで[Changeof Authorization CoA)]を発行できます。これにより、プロファイリングサービスは、すでに認証されているエンドポイントをより詳細に制御できます。

CoAタイプを構成するための設定の1つは、再認証」です。このオプションは、プロファイリング時に、すでに認証されているエンドポイントの再認証を強制するために使用されます。

参照：

b_ise_admin_guide_sample_chapter_010101.html

Cisco ISEでは、グローバルコンフィギュレーションで[ProfilerConfiguration]ページで[Changeof Authorization CoA)]を発行できます。これにより、プロファイリングサービスは、すでに認証されているエンドポイントをより詳細に制御できます。

CoAタイプを構成するための設定の1つは、再認証」です。このオプションは、プロファイリング時に、すでに認証されているエンドポイントの再認証を強制するために使用されます。

b_ise_admin_guide_sample_chapter_010101.html

質問: 382

Cisco AMP for Networksを使用する場合、分析のためにファイルをCiscoAMPクラウドにコピーする機能はどれですか。

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

正解: B ([コメントを發表する](#))

説明Spero分析では、実行可能ファイルのメタデータやヘッダー情報などの構造的特性を調べます。この情報に基づいてSpero署名を生成した後、ファイルが適格な実行可能ファイルである場合、デバイスはそれをAMPクラウドのSperoヒューリスティックエンジンに送信します。Speroシグネチャに基づいて、Speroエンジンはファイルがマルウェアであるかどうかを判断します。参照：

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide/v60/Reference_a_wrapper_Chapter_topic_here.html->Spero分析はの署名のみをアップロードします（実行可能ファイルをAMPクラウドに送信します。ファイル全体をアップロードするわけではありません。動的分析はファイルをAMPTThreatGridに送信します。Dynamic Analysisは、（全体の）ファイルをCisco Threat Grid（以前のAMP Threat Grid）に送信します。Cisco Threat Gridは、サンドボックス環境でファイルを実行し、ファイルの動作を分析してファイルが悪意のあるものであるかどうかを判断し、ファイルにマルウェアが含まれている可能性を示す脅威スコアを返します。脅威スコアから、割り当てられた脅威スコアの理由を含む動的分析の要約レポートを表示できます。また、Cisco Threat Gridを調べて、組織が送信したファイルの詳細なレポートや、組織が送信しなかったファイルの限られたデータを含むスクラブされたレポートを表示することもできます。ローカルマルウェア分析により、管理対象デバイスは、Cisco Talos Security Intelligence and Research Group (Talos)が提供する検出ルールセットを使用して、実行可能ファイル、PDF、オフィスドキュメント、およびその他のタイプのファイルで最も一般的なタイプのマルウェアをローカルで検査できます。ローカル分析はAMPクラウドにクエリを送信せず、ファイルを実行しないため、ローカルマルウェア分析は時間とシステムリソースを節約します。->マルウェア分析はファイルをどこにもアップロードせず、ファイルをローカルでチェックするだけです。サンドボックス分析機能はありません。これは、仮想マシンで疑わしいファイルを実行する動的分析の方法にすぎません。

Spero分析では、実行可能ファイルのメタデータやヘッダー情報などの構造的特性を調べます。この情報に基づいてSpero署名を生成した後、ファイルが適格な実行可能ファイルである場合、デバイスはそれをAMPクラウドのSperoヒューリスティックエンジンに送信します。Speroシグネチャに基づいて、Speroエンジンはファイルがマルウェアであるかどうかを判断します。

参照：

-> Spero分析は、（実行可能）ファイルの署名のみをAMPクラウドにアップロードします。ファイル全体をアップロードするわけではありません。動的分析はファイルをAMPTThreatGridに送信します。

Dynamic Analysisは、（全体の）ファイルをCisco Threat Grid（以前のAMP Threat Grid）に送信します。Cisco Threat Gridは、サンドボックス環境でファイルを実行し、ファイルの動作を分析してファイルが悪意のあるものであるかどうかを判断し、ファイルにマルウェアが含まれている可能性を示す脅威スコアを返します。脅威スコアから、割り当てられた脅威スコアの理由を含む動的分析の要約レポートを表示できます。また、Cisco Threat Gridを調べて、組織が送信したファイルの詳細なレポートや、組織が送信しなかったファイルの限られたデータを含むスクラブされたレポートを表示することもできます。

ローカルマルウェア分析により、管理対象デバイスは、Cisco Talos Security Intelligence and Research Group (Talos)が提供する検出ルールセットを使用して、実行可能ファイル、PDF、オフィスドキュメント、およびその他のタイプのファイルで最も一般的なタイプのマルウェアをローカルで検査できます。ローカル分析はAMPクラウドにクエリを送信せず、ファイルを実行しないため、ローカルマルウェア分析は時間とシステムリソースを節約します。->マルウェア分析はファイルをどこにもアップロードせず、ファイルをローカルでチェックするだけです。

サンドボックス分析機能はありません。これは、疑わしいファイルを実行する動的分析の方法にすぎません。説明Spero分析では、実行可能ファイルのメタデータやヘッダー情報などの構造的特性を調べます。この情報に基づいてSpero署名を生成した後、ファイルが適格な実行可能ファイルである場

合、デバイスはそれをAMPクラウドのSperoヒューリスティックエンジンに送信します。Speroシグネチャに基づいて、Speroエンジンはファイルがマルウェアであるかどうかを判断します。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero分析はの署名のみをアップロードします（実行可能ファイルをAMPクラウドに送信します。ファイル全体をアップロードするわけではありません。動的分析はファイルをAMPTreatGridに送信します。Dynamic Analysisは、（全体）ファイルをCisco Threat Grid（以前のAMP Threat Grid）に送信します。Cisco Threat Gridは、サンドボックス環境でファイルを実行し、ファイルの動作を分析してファイルが悪意のあるものであるかどうかを判断し、ファイルにマルウェアが含まれている可能性を示す脅威スコアを返します。脅威スコアから、割り当てられた脅威スコアの理由を含む動的分析の要約レポートを表示できます。また、Cisco Threat Gridを調べて、組織が送信したファイルの詳細なレポートや、組織が送信しなかったファイルの限られたデータを含むスクラブされたレポートを表示することもできます。ローカルマルウェア分析により、管理対象デバイスは、実行可能ファイル、PDF、オフィスドキュメント、およびその他のタイプのファイルをローカルで検査して、最も一般的なタイプのマルウェアを検出できます。Cisco Talos Security Intelligence and Research Group (Talos) が提供する検出ルールセットを使用します。ローカル分析はAMPクラウドにクエリを送信せず、ファイルを実行しないため、ローカルマルウェア分析は時間とシステムリソースを節約します。->マルウェア分析はファイルをどこにもアップロードせず、ファイルをローカルでチェックするだけです。サンドボックス分析機能はありません。これは、仮想マシンで疑わしいファイルを実行する動的分析の方法にすぎません。

質問: 383

VPN機能を左から右の説明にドラッグアンドドロップします。



正解:



質問: 384

基盤となるクラウドインフラストラクチャを管理または保守する必要なしに、クラウドコンシューマーがアプリケーションを開発および展開するための環境を提供するクラウドサービスモデルはどれですか？

- A. IaaS
- B. XaaS
- C. PaaS
- D. SaaS

正解: ([正解を表示します](#))

質問: **385**

Cisco Tetrationプラットフォームがユーザーの通常の動作を学習できるようにする疑わしいパターンはどれですか？

- A. ユーザーログインの疑わしい動作
- B. 興味深いファイルアクセス
- C. 特権の昇格
- D. 別のユーザーからのファイルアクセス

正解: **A** ([コメントを発表する](#))

質問: **386**

IPsecで使用する2つの暗号化アルゴリズムはどれですか？ 2つ選択してください)

- A. AES-BAC
- B. AES-ABC
- C. HMAC-SHA1 / SHA2
- D. トリプルAMC-CBC
- E. AES-CBC

正解: ([正解を表示します](#))

説明

説明

IPsecで使用するために定義された暗号化アルゴリズムには、次のものがあります。

+ HMAC-SHA1 / SHA2は、整合性の保護と信頼性を実現します。

+TripleDES-機密保持のためのCBC

+機密保持のためのAES-CBCおよびAES-CTR。

+AES-GCMとChaCha20-Poly1305は、機密性と認証を効率的に提供します。

質問: **387**

DNSトンネリングは、企業ネットワークからデータを盗み出すためにどのように使用されますか？

- A. 実際のIPアドレスを不正なアドレスに置き換えて情報を収集したり、他の攻撃を開始したりすることで、DNSサーバーを破壊します。
- B. 短い文字列に分割されたランダムな文字でペイロードをエンコードし、DNSサーバーが抽出されたデータを再構築します。
- C. DNS要求を、ユーザーの資格情報を盗むために使用される悪意のあるサーバーにリダイレクトします。これにより、ネットワークがさらに損傷したり盗まれたりする可能性があります。
- D. 再帰的なルックアップを許可してDNSサーバーを活用し、攻撃を他のDNSサーバーに拡散します。

正解: **B** ([コメントを発表する](#))

ドメインネームシステム (DNS)は、securitytut.comなどの人間にわかりやすいURLを183.33.24.13などのIPアドレスに変換するプロトコルです。DNSメッセージは各通信の開始としてのみ使用され、データ転送を目的としていないため、多くの組織はDNSトラフィックの悪意のあるアクティビティを

監視していません。その結果、DNSベースの攻撃は、ネットワークに対して開始された場合に効果的である可能性があります。DNSトンネリングはそのような攻撃の1つです。

DNSトンネリングの例を以下に示します。



- 攻撃者は、多くのオープンソースDNSトンネリングキットの1つを、信頼できるDNSネームサーバー (NS)と悪意のあるペイロードに組み込みます。
2. IPアドレス (例1.2.3.4)が攻撃者のインフラストラクチャから割り当てられ、ドメイン名 (例attackerdomain.com)が登録または再利用されます。レジストラは、トップレベルドメイン (.com)ネームサーバーに、attackerdomain.comへの要求を1.2.3.4にマップされたDNSレコードを持つ ns.attackerdomain.comに参照するように通知します。
- 3.攻撃者は、悪意のあるペイロードでシステムを侵害します。目的のデータが取得されると、ペイロードはデータを一連の32文字 (0-9、AZ)として短い文字列 \$KJ242AIE9、P028X977W、...)に分割してエンコードします。
- 4.ペイロードは、ドメイン名の一部として各文字列を使用して、攻撃者のドメインに対して何千もの一意のDNSレコード要求を開始します (例：3KJ242AIE9.attackerdomain.com)。攻撃者の忍耐力とステルス性に応じて、疑わしいネットワークアクティビティを回避するために、要求を数日または数か月にわたって間隔を空けることができます。5.要求は再帰DNSリゾルバーに転送されます。解決中に、要求は攻撃者の権限のあるDNSネームサーバーに送信されます。6.トンネリングキットは、エンコードされた文字列を解析し、盗み出されたデータを再構築します。参照 <https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0>
- 5.要求は再帰DNSリゾルバーに転送されます。解決中に、要求は攻撃者の権限のあるDNSネームサーバーに送信されます。
- 6.トンネリングキットは、エンコードされた文字列を解析し、抽出されたデータを再構築します。
- ドメイン名の一部 (例3KJ242AIE9.attackerdomain.com)。攻撃者の忍耐力とステルス性に応じて、疑わしいネットワークアクティビティを回避するために、要求を数日または数か月にわたって間隔を空けることができます。5.要求は再帰DNSリゾルバーに転送されます。解決中に、要求は攻撃者の権限のあるDNSネームサーバーに送信されます。6.トンネリングキットは、エンコードされた文字列を解析し、盗み出されたデータを再構築します。参照：<https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0>

質問: 388

crypto isakmp key ciscXXXXXXXXX address 172.16.0.0コマンドを実行した結果はどうなりますか？

- A. キーciscXXXXXXXXXを使用して、172.16.0.0/16の範囲のIKEv2ピアを認証します
- B. キーciscXXXXXXXXXを使用して、172.16.0.0/32ピアのIPアドレスを認証します
- C. キーciscXXXXXXXXXを使用して、172.16.0.0/16の範囲のIKEv1ピアを認証します
- D. キーciscXXXXXXXXXを使用して、IKEExchange内のすべての証明書を保護します

正解: A ([コメントを发表する](#))

上記のコマンドの構文は次のとおりです。cryptoisakmpkeyenc-type-digit kestring {address peer-address [mask] | ipv6 ipv6-address / ipv6-prefix | hostname hostname} [no-xauth] peer-address引数は、リモートピアのIPアドレスまたはIPv6アドレスを指定します。参照：

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp6039879000> crypto isakmp key enc-type-digit kestring {address peer-address [mask] | ipv6 ipv6-address / ipv6-prefix | hostname hostname} [no-xauth] peer-address引数は、リモートピアのIPアドレスまたはIPv6アドレスを指定します。

上記のコマンドの構文は次のとおりです。cryptoisakmpkeyenc-type-digit keystore {address peer-address [mask] | ipv6 ipv6-address / ipv6-prefix | hostname hostname} [no-xauth] peer-address引数は、リモートピアのIPアドレスまたはIPv6アドレスを指定します。参照：
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp6039879000>

質問: 389

ASAファイアウォール透過モードのブリッジグループの特徴は何ですか。

- A. 複数のインターフェースが含まれ、インターフェース間のアクセスルールはカスタマイズ可能
- B. これはレイヤー3セグメントであり、1つのポートとカスタマイズ可能なアクセスルールが含まれています
- C. 単一のアクセスルールでARPトラフィックを許可します
- D. BVIインターフェースにIPアドレスがあり、管理トラフィックに使用されます

正解: **A** ([コメントを发表する](#))

ブリッジグループは、ASAがルートの代わりにブリッジするインターフェイスのグループです。ブリッジグループは、透過ファイアウォールモードでのみサポートされます。他のファイアウォールインターフェイスと同様に、インターフェイス間のアクセス制御が制御され、通常のファイアウォールチェックがすべて実行されます。各ブリッジグループには、Bridge Virtual Interface (BVI)が含まれています。ASAは、ブリッジグループから発信されたパケットの送信元アドレスとしてBVIIPアドレスを使用します。BVI IPアドレスは、ブリッジグループメンバーインターフェイスと同じサブネット上にある必要があります。BVIは、セカンダリネットワーク上のトラフィックをサポートしていません。BVIIPアドレスと同じネットワーク上のトラフィックのみがサポートされます。ブリッジグループごとに複数のインターフェイスを含めることができます。ブリッジグループごとに3つ以上のインターフェイスを使用する場合、同じネットワーク上の複数のセグメント間の通信を制御できます。内側と外側の間だけではありません。たとえば、相互に通信したくない3つの内部セグメントがある場合、各セグメントを別々のインターフェイスに配置し、それらが外部インターフェイスとのみ通信できるようにすることができます。または、インターフェイス間のアクセスルールをカスタマイズして、必要な数のアクセスのみを許可することもできます。参照：

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html>注 BVIインターフェイスは使用されません管理目的で。ただし、ブリッジグループの一部ではなく、ASAへの管理トラフィックのみを許可する個別の管理スロット/ポートインターフェイスを追加できます。そして、それらが外部インターフェイスと通信することだけを許可します。または、インターフェイス間のアクセスルールをカスタマイズして、必要な数のアクセスのみを許可することもできます。参照：

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html>注 BVIインターフェイスは使用されません管理目的で。ただし、ブリッジグループの一部ではなく、ASAへの管理トラフィックのみを許可する個別の管理スロット/ポートインターフェイスを追加できます。

透過ファイアウォールモードでサポートされています。他のファイアウォールインターフェイスと同様に、インターフェイス間のアクセス制御が制御され、通常のファイアウォールチェックがすべて実行されます。
各ブリッジグループには、Bridge Virtual Interface (BVI)が含まれています。ASAは、ブリッジグループから発信されたパケットの送信元アドレスとしてBVIIPアドレスを使用します。BVI IPアドレスは、ブリッジグループメンバーインターフェイスと同じサブネット上にある必要があります。BVIは、セカンダリネットワーク上のトラフィックをサポートしていません。BVIIPアドレスと同じネットワーク上のトラフィックのみがサポートされます。
ブリッジグループごとに複数のインターフェイスを含めることができます。ブリッジグループごとに3つ以上のインターフェイスを使用する場合は、内部と外部の間だけでなく、同じネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互に通信したくない3つの内部セグメントが

ある場合、各セグメントを別々のインターフェイスに配置し、それらが外部インターフェイスとのみ通信できるようにすることができます。または、インターフェイス間のアクセスルールをカスタマイズして、必要な数のアクセスのみを許可することもできます。

参照：

ブリッジグループは、ASAがルートの代わりにブリッジするインターフェイスのグループです。ブリッジグループは、透過ファイアウォールモードでのみサポートされます。他のファイアウォールインターフェイスと同様に、インターフェイス間のアクセス制御が制御され、通常のファイアウォールチェックがすべて実行されます。各ブリッジグループには、Bridge Virtual Interface (BVI)が含まれています。ASAは、ブリッジグループから発信されたパケットの送信元アドレスとしてBVIIPアドレスを使用します。BVI IPアドレスは、ブリッジグループメンバーインターフェイスと同じサブネット上にある必要があります。BVIは、セカンダリネットワーク上のトラフィックをサポートしていません。BVIIPアドレスと同じネットワーク上のトラフィックのみがサポートされます。ブリッジグループごとに複数のインターフェイスを含めることができます。ブリッジグループごとに3つ以上のインターフェイスを使用する場合、同じネットワーク上の複数のセグメント間の通信を制御できます。内側と外側の間だけではありません。たとえば、相互に通信したくない3つの内部セグメントがある場合、各セグメントを別々のインターフェイスに配置し、それらが外部インターフェイスとのみ通信できるようにすることができます。または、インターフェイス間のアクセスルールをカスタマイズして、必要な数のアクセスのみを許可することもできます。参照：

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html>注：BVIインターフェイスは使用されません管理目的で。ただし、ブリッジグループの一部ではなく、ASAへの管理トラフィックのみを許可する個別の管理スロット/ポートインターフェイスを追加できます。そして、それらが外部インターフェイスと通信することだけを許可します。または、インターフェイス間のアクセスルールをカスタマイズして、必要な数のアクセスのみを許可することもできます。参照：

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html>注：BVIインターフェイスは使用されません管理目的で。ただし、ブリッジグループの一部ではなく、ASAへの管理トラフィックのみを許可する個別の管理スロット/ポートインターフェイスを追加できます。

質問: 390

SaaSベースのアプリケーションを保護するには何を有効にする必要がありますか？

- A. 2要素認証
- B. エンドツーエンド暗号化
- C. アプリケーションセキュリティゲートウェイ
- D. モジュラーポリシーフレームワーク

正解: ([正解を表示します](#))

質問: 391

Flexible NetFlowレコードの2つの利点は何ですか？ (2つ選択してください)

- A. ユーザーがフロー情報を構成してカスタマイズされたトラフィック識別を実行できるようにします
- B. トラフィックをドロップすることで攻撃を防止します
- C. アカウンティングと請求の機能強化を提供します
- D. 複数の会計技術を1つの会計メカニズムに統合します
- E. レイヤー2から4までの幅広いIPパケット情報の監視を提供します

正解: A,C ([コメントを發表する](#))

NetFlowは通常、次のようないくつかの主要な顧客アプリケーションに使用されます。

…。

請求と会計。NetFlowデータは、非常に柔軟で詳細なリソース使用率アカウンティングのために、きめ細かいメータリング（たとえば、フローデータにはIPアドレス、パケット数とバイト数、タイムスタンプ、サービスの種類（ToS）、アプリケーションポートなどの詳細が含まれます）を提供します。サービスプロバイダーは、時刻、帯域幅の使用量、アプリケーションの使用量、サービス品質などに基づいて請求に情報を使用する場合があります。企業のお客様は、この情報を部門のチャージバックまたはリソース使用率のコスト配分に使用できます。

NetFlowは通常、次のようないくつかの主要な顧客アプリケーションに使用されます。

…。

請求と会計。NetFlowデータは、非常に柔軟で詳細なリソース使用率アカウンティングのために、きめ細かいメータリング（たとえば、フローデータにはIPアドレス、パケット数とバイト数、タイムスタンプ、サービスの種類（ToS）、アプリケーションポートなどの詳細が含まれます）を提供します。サービスプロバイダーは、時刻、帯域幅の使用量、アプリケーションの使用量、サービス品質などに基づいて請求に情報を使用する場合があります。企業のお客様は、この情報を部門のチャージバックまたはリソース使用率のコスト配分に使用できます。

参照：

事前定義されたFlexibleNetFlowレコードがトラフィック要件に適していない場合は、Flexible NetFlowの収集および一致コマンドを使用してユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来の

NetFlowでは、レイヤー2から4までを監視できますが、FlexibleNetFlowはこれらのレイヤーを超えています。

NetFlowは通常、次のようないくつかの主要な顧客アプリケーションに使用されます。

…。

請求と会計。NetFlowデータは、非常に柔軟で詳細なリソース使用率アカウンティングのために、きめ細かいメータリング（たとえば、フローデータにはIPアドレス、パケット数とバイト数、タイムスタンプ、サービスの種類（ToS）、アプリケーションポートなどの詳細が含まれます）を提供します。サービスプロバイダーは、時刻、帯域幅の使用量、アプリケーションの使用量、サービス品質などに基づいて請求に情報を使用する場合があります。企業のお客様は、この情報を部門のチャージバックまたはリソース使用率のコスト配分に使用できます。

事前定義されたFlexibleNetFlowレコードがトラフィック要件に適していない場合は、Flexible NetFlowの収集および一致コマンドを使用してユーザー定義（カスタム）レコードを作成できます。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来の

NetFlowではレイヤー2から4までの監視が可能です。Flexible NetFlowはこれらを超えています。事前定義されたFlexibleNetFlowレコードがトラフィック要件に適していない場合は、柔軟なNetFlow収集および照合コマンド。カスタマイズされたレコードを作成する前に、キーフィールドと非キーフィールドに使用する基準を決定する必要があります。

cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997注：従来の

NetFlowでは、レイヤー2から4までを監視できますが、FlexibleNetFlowはこれらのレイヤーを超えています。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード：**JPNshiken**」

質問: 392

電子メールおよびWebトラフィックのIPアドレスのレピュテーションを追跡できるTalosレピュテーションセンターはどれですか？

- A. IPおよびドメインレピュテーションセンター
- B. IPブラックリストセンター
- C. AMPレピュテーションセンター
- D. ファイルレピュテーションセンター

正解: [\(正解を表示します\)](#)

質問: 393

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fald	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5a5	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e14	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d66	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62e1.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

展示を参照してください。この出力を生成し、どのポートがdot1xまたはmabで認証されているかを示すために使用されたコマンドはどれですか。

- A. dot1xallを表示
- B. 認証方法を表示
- C. 認証登録を表示する
- D. 認証セッションを表示

正解: [\(正解を表示します\)](#)

質問: 394

組織は、ネットワーク上にマイクロセグメンテーションを実装しようとしており、ネットワーク内のアプリケーションの可視性を取得できるようにしたいと考えています。ソリューションは、コンプライアンスを維持および強制できる必要があります。これらの要件を満たすためにどの製品を使用する必要がありますか？

- A. Cisco Umbrella
- B. Cisco AMP
- C. Cisco Stealthwatch
- D. Cisco Tetration

正解: [\(正解を表示します\)](#)

マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。

Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。

正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。

マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。

Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。

正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。

マイクロセグメンテーションは、特定のアプリケーショントラフィックを明示的に許可し、デフォルトで他のすべてのトラフィックを拒否することにより、アプリケーションを保護します。マイクロセグメンテーションは、データセンターとクラウドのアプリケーションワークロードにゼロトラストセキュリティモデルを実装するための基盤です。

Cisco Tetrationは、あらゆるインフラストラクチャおよびあらゆるクラウドにわたってコンピューティングインスタンスを保護するように設計されたアプリケーションワークロードセキュリティプラットフォームです。これを実現するために、動作と属性駆動型のマイクロセグメンテーションポリシーの生成と実施を使用します。さまざまなシステムからの自動化された網羅的なコンテキストを通じて信頼できるアクセスを可能にし、セキュリティポリシーを自動的に適応させます。

正確なマイクロセグメンテーションポリシーを生成するために、Cisco Tetrationはアプリケーション依存関係マッピングを実行して、さまざまなアプリケーション層とインフラストラクチャサービス間の関係を検出します。さらに、このプラットフォームは、リアルタイムデータまたは履歴データを使用した「What-if」ポリシー分析をサポートし、ポリシーアプリケーションの事前施行の検証とリスク評価を支援して、継続的なアプリケーションの可用性を確保します。正規化されたマイクロセグメンテーションポリシーは、アプリケーションワークロード自体を介して適用できるため、パブリッククラ

ウドやデータセンターで実行されている仮想化、ベアメタル、コンテナのワークロードなど、あらゆる環境でワークロードのマイクロセグメンテーションに一貫したアプローチをとることができます。マイクロセグメンテーションポリシーが適用されると、Cisco Tetrationはコンプライアンスの逸脱を監視し続けます。

質問: 395

組織がエンドポイントのパッチ適用戦略を持つことが重要なのはなぜですか？

- A. 既存のバグが発生したときにネットワーク管理者に通知されるようにします
- B. 内部PSIRT組織は最新のバグを認識しています
- C. 組織がエンドポイントの脆弱性を特定できるようにする
- D. 最新のセキュリティ修正がエンドポイントにインストールされます

正解: **A** ([コメントを發表する](#))

質問: 396

Cisco Tetrationプラットフォームがユーザーの通常の動作を学習できるようにする疑わしいパターンはどれですか？

- A. 別のユーザーからのファイルアクセス
- B. 興味深いファイルアクセス
- C. ユーザーログインの疑わしい動作
- D. 特権の昇格

正解: ([正解を表示します](#))

説明説明現在のリリースでCisco Tetrationプラットフォームが調べるさまざまな疑わしいパターンは次のとおりです。+シェルコードの実行 :シェルコードで使用されるパターンを探します。+特権の昇格 :プロセス系統ツリーで、特権が低い特権から高い特権に変更されるのを監視します。+サイドチャネル攻撃 :Cisco Tetrationプラットフォームは、キャッシュタイミング攻撃とページテーブル障害バーストを監視します。これらを使用して、Meltdown、Spectre、およびその他のキャッシュタイミング攻撃を検出できます。+Rawソケットの作成 : 非標準のプロセス (pingなど)によるrawソケットの作成。+ユーザーログインの疑わしい動作 :Cisco Tetrationプラットフォームは、ユーザーログインの失敗とユーザーログイン方法を監視します。+興味深いファイルアクセス :Cisco Tetrationプラットフォームは、機密ファイルを調べるために武装することができます。+別のユーザーからのファイルアクセス :Cisco Tetrationプラットフォームは、どのファイルがどのユーザーによってアクセスされるかの通常の動作を学習します。+見えないコマンド :Cisco Tetrationプラットフォームは、コマンドの動作とセット、および各コマンドの系統を経時的に学習します。新しいコマンドまたは異なる系統のコマンドは、TetrationAnalyticsプラットフォームの関心を引き起こします。参照 :<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html>説明Cisco Tetrationプラットフォームのさまざまな疑わしいパターン現在のリリースの外観は次のとおりです。新しいコマンドまたは異なる系統のコマンドは、TetrationAnalyticsプラットフォームの関心を引き起こします。参照 :<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html>説明Cisco Tetrationプラットフォームのさまざまな疑わしいパターン現在のリリースの外観は次のとおりです。+シェルコードの実行 :シェルコードで使用されるパターンを探します。+特権の昇格 :プロセス系統ツリーで、特権が低い特権から高い特権に変更されるのを監視します。+サイドチャネル攻撃 :Cisco Tetrationプラットフォームは、キャッシュタイミング攻撃とページテーブル障害バーストを監視します。これらを使用して、Meltdown、Spectre、およびその他のキャッシュタイミング攻撃を検出できます。+Rawソケットの作成 : 非標準のプロセス (pingなど)によるrawソケットの作成。+ユーザーログインの疑わしい動作 :Cisco Tetrationプラットフォームは、ユーザーログインの失敗とユーザーログイン方法を監視します。

+興味深いファイルアクセス :Cisco Tetrationプラットフォームは、機密ファイルを調べるために武装することができます。

+別のユーザからのファイルアクセス :Cisco Tetrationプラットフォームは、どのユーザがどのファイルにアクセスするかの通常の動作を学習します。

+見えないコマンド :Cisco Tetrationプラットフォームは、コマンドの動作とセット、および各コマンドの系統を経時的に学習します。新しいコマンドまたは異なる系統のコマンドは、TetrationAnalyticsプラットフォームの関心を引き起こします。

説明説明現在のリリースでCisco Tetrationプラットフォームが調べるさまざまな疑わしいパターンは次のとおりです。

- +シェルコードの実行 :シェルコードで使用されるパターンを探します。
- +特権の昇格 :プロセス系統ツリーで、特権が低い特権から高い特権に変更されるのを監視します。
- +サイドチャネル攻撃 :Cisco Tetrationプラットフォームは、キャッシュタイミング攻撃とページテーブル障害バーストを監視します。これらを使用して、Meltdown、Spectre、およびその他のキャッシュタイミング攻撃を検出できます。
- +Rawソケットの作成 :非標準のプロセス (pingなど) によるrawソケットの作成。
- +ユーザーログインの疑わしい動作 :Cisco Tetrationプラットフォームは、ユーザーログインの失敗とユーザーログイン方法を監視します。
- +興味深いファイルアクセス :Cisco Tetrationプラットフォームは、機密ファイルを調べるために武装することができます。
- +別のユーザーからのファイルアクセス :Cisco Tetrationプラットフォームは、どのファイルがどのユーザーによってアクセスされるかの通常の動作を学習します。
- +見えないコマンド :Cisco Tetrationプラットフォームは、コマンドの動作とセット、および各コマンドの系統を経時的に学習します。新しいコマンドまたは異なる系統のコマンドは、TetrationAnalyticsプラットフォームの関心を引き起こします。

参照 :<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html>

質問: 397

組織はCisco FMCを使用して、複数のCisco FTDデバイスを一元管理します。デフォルトの管理ポートはネットワーク上の他の通信と競合するため、変更する必要があります。すべてのデバイスが相互に通信できるようにするには、何をする必要がありますか？

- A. Cisco FMCおよびすべての管理対象Cisco FTDデバイスの管理ポートを手動で変更します
- B. Cisco FTDを通過するようにトンネルを設定します
- C. Cisco FMCの管理ポートを変更して、管理対象のすべてのCisco FTDデバイスに変更をプッシュします。
- D. トンネルポートを8305に設定します

FMCと管理対象デバイスは、SSLで暗号化された双方向の通信チャネルを使用して通信します。このチャネルはデフォルトでポート8305にあります。

正解: ([正解を表示します](#))

リモート管理ポートのデフォルト設定を維持することを強くお勧めしますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、相互に通信する必要がある展開内のすべてのデバイスに対して管理ポートを変更する必要があります。

質問: 398

NetFlowフローモニタリングの2つの機能は何ですか？ 2つ選択してください。)

- A. マルチキャスト、MPLS、またはブリッジトラフィックの追跡に使用できます。
- B. 入力および出力情報を追跡できます
- C. フローレコードとフローインポーターを含める
- D. すべての入力フロー情報をインターフェースにコピーします
- E. インターフェイスでのパケットサンプリングは必要ありません

正解: ([正解を表示します](#))

質問: 399

ブルートフォース攻撃に対して最高レベルの保護を提供するアルゴリズムのタイプはどれですか？

- A. PFS
- B. MD5

- C. SHA
- D. HMAC

正解: [\(正解を表示します\)](#)

質問: 400

NetFlowエクスポートフォーマットを左から右の説明にドラッグアンドドロップします。

Version 1	appropriate only for the main cache
Version 5	introduced support for aggregation caches
Version 8	appropriate only for legacy systems
Version 9	introduced extensibility

正解:

Version 1	Version 5	
Version 5	Version 8	es
Version 8	Version 1	
Version 9	Version 9	

質問: 401

最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

- A. アクセスポリシーを変更します。
- B. 識別プロファイルを変更します。
- C. アウトバウンドマルウェアスキャンポリシーを変更する
- D. Webプロキシ設定を変更する

正解: D [\(コメントを发表する\)](#)

参照：

An explicit proxy deployment is when a client proxy-aware application, like a mature web browser, has a configuration area within for proxy settings to declare and use a proxy, like the WSA. This method is typically combined with a firewall restricting web traffic that does not originate from the WSA's IP to prevent users from circumventing web policy controls and accessing

質問: 402

最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

- A. アクセスポリシーを変更する
- B. 識別プロファイルを変更する
- C. アウトバウンドマルウェアスキャンポリシーを変更する
- D. Webプロキシ設定を変更する

正解: A ([コメントを发表する](#))

アクセス制御ルールのURL条件を使用すると、ネットワーク上のユーザーがアクセスできるWebサイトを制限できます。この機能はURLフィルタリングと呼ばれます。アクセス制御を使用してブロックする または逆に許可する)URLを指定する方法は2つあります。-任意のライセンスで、個々のURL、URLのグループ、およびURLリストとフィードを手動で指定して、きめ細かいカスタムを実現できます。Webトラフィックの制御。-URLフィルタリングライセンスを使用すると、URLの一般的な分類またはカテゴリ、リスクレベル、またはレピュテーションに基づいてWebサイトへのアクセスを制御することもできます。システムは、このカテゴリとレピュテーションデータを接続ログ、侵入イベント、およびアプリケーションの詳細に表示します。カテゴリとレピュテーションデータを使用すると、ポリシーの作成と管理も簡素化されます。これにより、システムがWebトラフィックを期待どおりに制御することが保証されます。最後に、シスコの脅威インテリジェンスは、新しいURL、および既存のURLの新しいカテゴリとリスクで継続的に更新されるため、システムが最新の情報を使用して要求されたURLをフィルタリングできるようにすることができます。マルウェア、スパム、ボットネット、フィッシングなどのセキュリティの脅威を表す悪意のあるサイトは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html また、フィッシングは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html また、フィッシングは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html

-どのライセンスでも、個々のURL、URLのグループ、およびURLリストとフィードを手動で指定して、Webトラフィックをきめ細かくカスタム制御できます。

-URLフィルタリングライセンスを使用すると、URLの一般的な分類またはカテゴリ、リスクレベル、またはレピュテーションに基づいてWebサイトへのアクセスを制御することもできます。システムは、このカテゴリとレピュテーションデータを接続ログ、侵入イベント、およびアプリケーションの詳細に表示します。

カテゴリとレピュテーションデータを使用すると、ポリシーの作成と管理も簡素化されます。これにより、システムがWebトラフィックを期待どおりに制御することが保証されます。最後に、シスコの脅威インテリジェンスは、新しいURL、および既存のURLの新しいカテゴリとリスクで継続的に更新されるため、システムが最新の情報を使用して要求されたURLをフィルタリングできるようにすることができます。マルウェア、スパム、ボットネット

ト、フィッシングなどのセキュリティの脅威を表す悪意のあるサイトは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。

アクセス制御ルールのURL条件を使用すると、ネットワーク上のユーザーがアクセスできるWebサイトを制限できます。この機能はURLフィルタリングと呼ばれます。アクセス制御を使用してブロックする または逆に許可する)URLを指定する方法は2つあります。-任意のライセンスで、個々のURL、URLのグループ、およびURLリストとフィードを手動で指定して、きめ細かいカスタムを実現できます。Webトラフィックの制御。-URLフィルタリングライセンスを使用すると、URLの一般的な分類またはカテゴリ、リスクレベル、またはレピュテーションに基づいてWebサイトへのアクセスを制御することもできます。システムは、このカテゴリとレピュテーションデータを接続ログ、侵入イベント、およびアプリケーションの詳細に表示します。カテゴリとレピュテーションデータを使用すると、ポリシーの作成と管理も簡素化されます。これにより、システムがWebトラフィックを期待どおりに制御することが保証されます。最後に、シスコの脅威インテリジェンスは、新しいURL、および既存のURLの新しいカテゴリとリスクで継続的に更新されるため、システムが最新の情報を使用して要求されたURLをフィルタリングできるようにすることができます。マルウェア、スパム、ボットネット、フィッシングなどのセキュリティの脅威を表す悪意のあるサイトは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html また、フィッシングは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html また、フィッシングは、新しいポリシーを更新して展開するよりも早く現れたり消えたりする可能性があります。参照 https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html

質問: 403

エンドポイントのセキュリティを確保するために、Cisco IdentityServicesEngineポスチャモジュールが提供する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. エンドポイントサブリカント構成がデプロイされます。
- B. パッチ管理の修正を行います。
- C. エンドポイントグループへの割り当ては、エンドポイント属性に基づいて動的に行われます。
- D. アクセスが許可される前に、最新のウイルス対策アップデートが適用されます。
- E. 集中管理ソリューションが導入されています。

正解: ([正解を表示します](#))

質問: 404

ゲストサービスのISEへの認証のためにユーザーをWebポータルにリダイレクトするために使用される2つのメカニズムは何ですか？ 2つ選択してください。)

- A. シングルサインオン
- B. TACACS +
- C. ローカルWeb認証
- D. 中央Web認証
- E. 多因子認証

正解: ([正解を表示します](#))

質問: 405

Cisco Email Securityの2つの機能のうち、電子メールの脅威から組織を保護できるのはどれですか。 2つ選択してください)

- A. 時間ベースのワンタイムパスワード
- B. データ損失防止
- C. ヒューリスティックベースのフィルタリング
- D. ジオロケーションベースのフィルタリング
- E. NetFlow

正解: ([正解を表示します](#))

説明データ損失防止 (DLP)と使いやすい電子メール暗号化をすべて1つのソリューションでを使用して、送信電子メールの機密コンテンツを保護します。Cisco Email Securityアプライアンスは、特定の地域からの着信メール接続と着信メッセージを処理し、それらに対して適切なアクションを実行できるようになりました。たとえば、次のようになります。-特定の地域からの電子メールの脅威を防止します。-特定の地域からのメールを許可または禁止します。参照 :https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide/fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.htmlデータ損失防止 (DLP)を使用して送信メールの機密コンテンツを保護する使いやすい電子メール暗号化をすべて1つのソリューションにまとめました。

Cisco Email Securityアプライアンスは、特定の地理的位置からの着信メール接続と着信メッセージを処理し、それらに対して適切なアクションを実行できるようになりました。たとえば、次のようになります。

-特定の地理的地域からの電子メールの脅威を防ぎます。

-特定の地域からのメールを許可または禁止します。

参照 :

説明データ損失防止 (DLP)と使いやすい電子メール暗号化をすべて1つのソリューションでを使用して、送信電子メールの機密コンテンツを保護します。Cisco Email Securityアプライアンスは、特定の地域からの着信メール接続と着信メッセージを処理し、それらに対して適切なアクションを実行できるようになりました。たとえば、次のようになります。-特定の地域からの電子メールの脅威を防止します。-特定の地域からのメールを許可または禁止します。参照 :https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide/fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

質問: 406

Cisco Stealthwatch Cloudはどのようにクラウド環境にセキュリティを提供しますか？

- A. 可視性と脅威の検出を提供します。
- B. 機密データの漏洩を防ぎます。
- C. クライアントとサーバーにインターネットベースのDNS保護を割り当てます。
- D. パブリックネットワークとプライベートネットワーク間の安全な接続を容易にします。

正解: ([正解を表示します](#))

説明Cisco Stealthwatch Cloud (Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)などのパブリッククラウドインフラストラクチャ内で可視性と脅威の検出を提供するSaaS製品として利用できます。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 407

オンプレミスではない環境での侵害、アプリケーションリスク、およびデータ侵害を削減するのに役立つCiscoAPIベースのブローカとは何ですか。

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco AMP
- D. Cisco App Dynamics

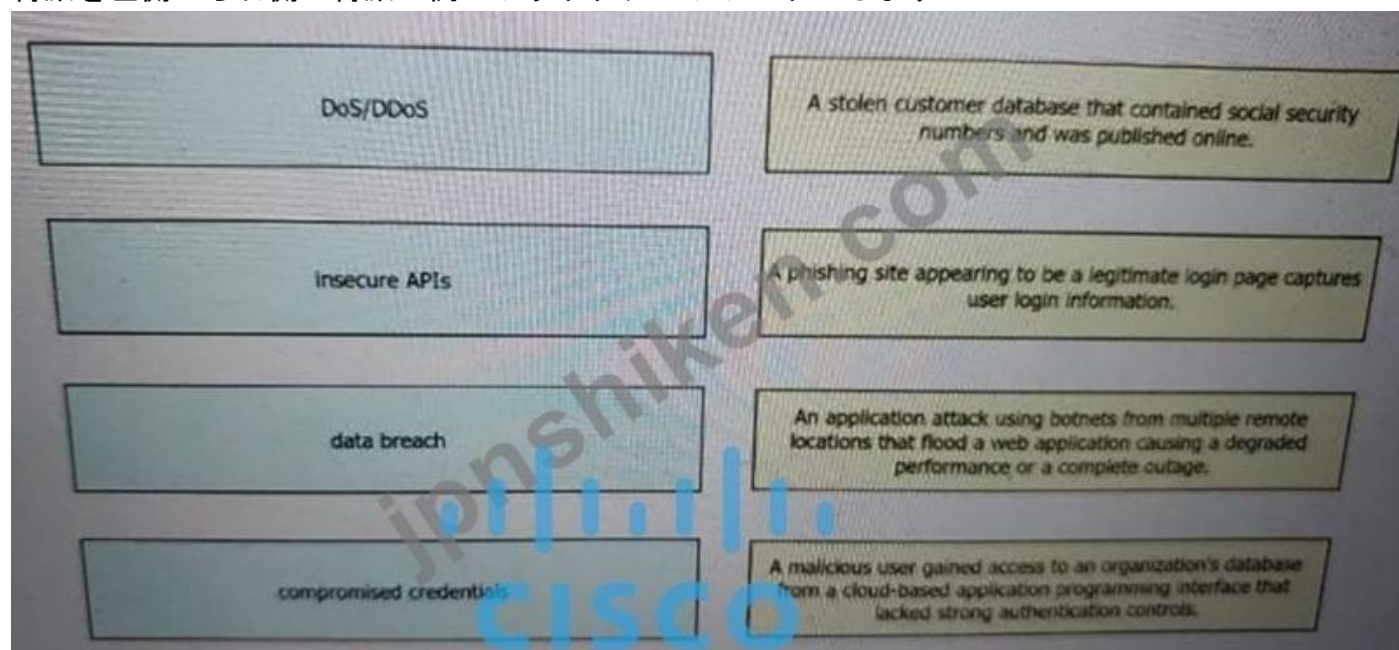
正解: A ([コメントを发表する](#))

説明

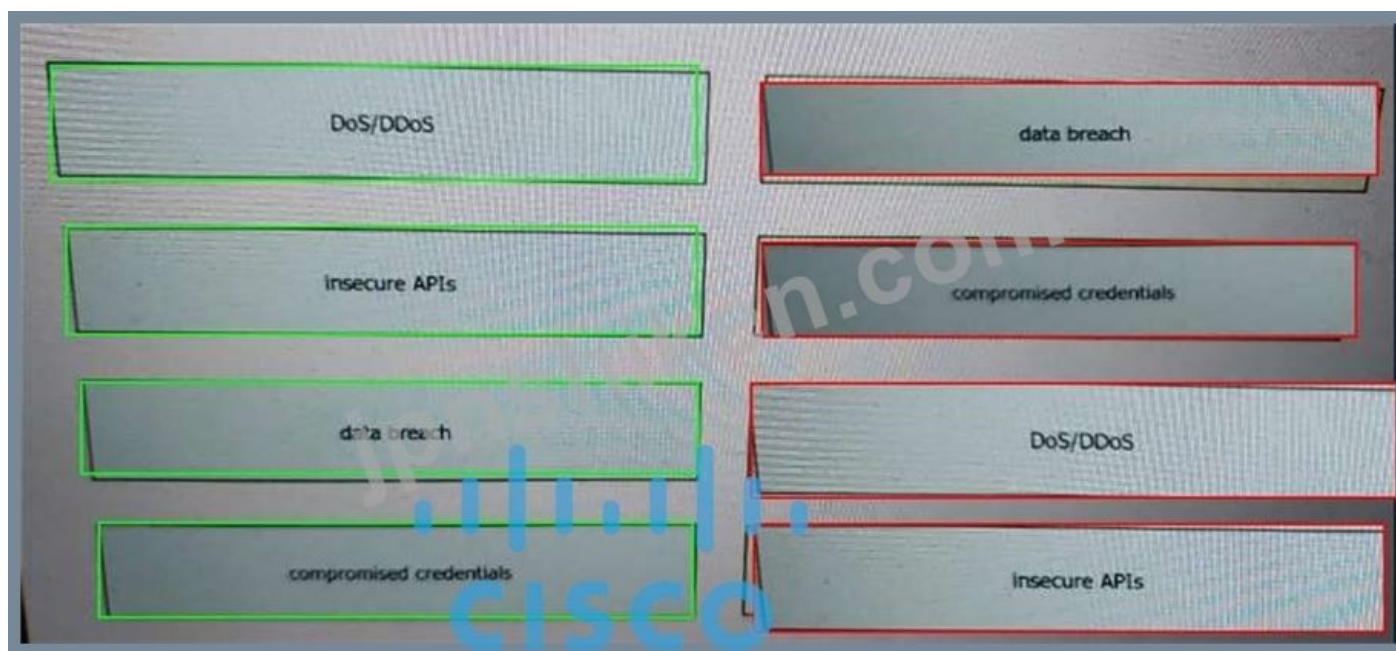
Cisco Cloudlock is the API-based cloud access security broker (CASB) that helps accelerate use of the cloud. By securing your identities, data, and apps, Cloudlock combats account compromises, breaches, and cloud app ecosystem risks. Our API-driven approach provides a simple and open way to enable healthy cloud adoption.

質問: 408

脅威を左側から右側の脅威の例にドラッグアンドドロップします



正解:



質問: 409

シスコ内のどのグループが週刊ニュースレターを作成および発行して、サイバーセキュリティの専門家が進行中の最も蔓延している脅威を認識し続けるのを支援していますか？

- A. PSIRT
- B. タロス
- C. CSIRT
- D. DEVNET

正解: (正解を表示します)

Talos Threat Sourceは、Cisco Talosからの定期的なインテリジェンスアップデートであり、毎週最大の脅威やその他のセキュリティニュースを強調しています。参照 <https://talosintelligence.com/newsletters> Talos Threat Sourceは、Cisco Talosからの定期的なインテリジェンスアップデートであり、毎週最大の脅威やその他のセキュリティニュースに焦点を当てています。参照 <https://talosintelligence.com/newsletters>

質問: 410

Cisco Application Visibility and Controlを使用して、ユーザがアプリケーションの使用状況とパフォーマンスの統計をエクスポートできるサービスはどれですか。

- A. SNORT
- B. NetFlow
- C. SNMP
- D. 802.1X

正解: B (コメントを发表する)

アプリケーションの可視性と制御 (AVC)は、アプリケーションの使用状況とパフォーマンスの統計をエクスポートするためにNetFlowをサポートします。このデータは、分析、請求、およびセキュリティポリシーに使用できます。

質問: 411

Cisco Security Managerは何を管理していますか？

- A. WSA

- B. ASA
- C. アクセスポイントO
- D. ESA

正解: ([正解を表示します](#))

説明

<https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html>

質問: 412

Cisco AMPforEndpointsをネットワークにインストールする利点は何ですか。

- A. セキュリティのためにエンドポイントにオペレーティングシステムのパッチを提供します。
- B. エンドポイントのネットワーク接続にフローベースの可視性を提供します。
- C. アプリケーション制御とリアルタイムスキャンを通じてエンドポイントシステムを保護します。
- D. エンドポイントに動作分析を使用できるようにします。

正解: C ([コメントを發表する](#))

参照 :

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance-c45-731874.html>

質問: 413

ネットワーク上で現在発生していることに対する可視性と認識を提供するものは何ですか？

- A. テレメトリ
- B. プライムインフラストラクチャ
- C. CMX
- D. WMI

正解: ([正解を表示します](#))

質問: 414

AMP for Endpoints Outbreak Control内の2つのリストタイプは何ですか？ 2つ選択してください。）

- A. ブロックされたポート
- B. 単純なカスタム検出
- C. コマンドアンドコントロール
- D. 許可されたアプリケーション
- E. URL

正解: B,D ([コメントを發表する](#))

説明/リファレンス <https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf>第2章

質問: 415

ネットワークエンジニアは、FlexVPNとDMVPNのどちらが環境に適しているかを把握しようとしています。

それらには、接続のためのより厳格なセキュリティ、複数のセキュリティアソシエーション、より効率的なVPN確立、およびより少ない帯域幅の消費が必要です。これに最適なソリューションとその理由は何ですか？

- A. DMVPNはIKEv2をサポートし、FlexVPNはサポートしないため

- B. FlexVPNはIKEv2をサポートし、DMVPNはサポートしないため
- C. 複数のSAを使用し、DMVPNは使用しないため、FlexVPN
- D. DMVPNは複数のSAを使用し、FlexVPNは使用しないため

正解: ([正解を表示します](#))

説明

FlexVPNはIKEv2->回答Aをサポートしていますが正しくありません。

DMVPNはIKEv1とIKEv2-の両方をサポートします-回答Bは正しくありません。

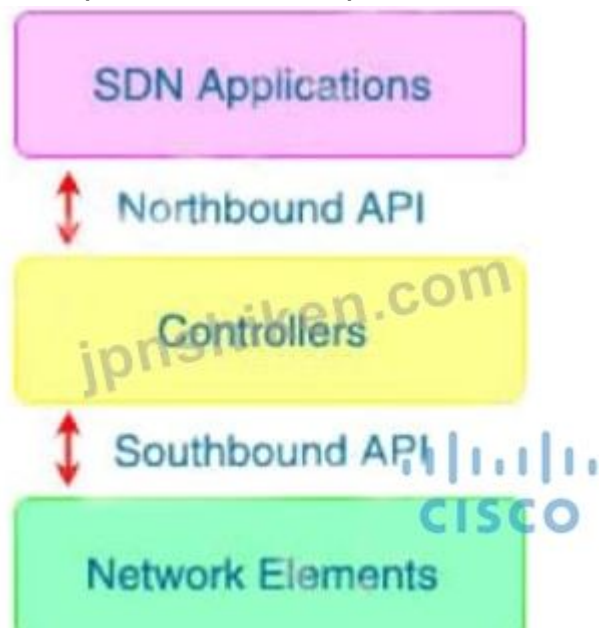
FlexVPNは複数のSAをサポートします-回答Dは正しくありません。

質問: 416

ソフトウェア定義ネットワークアーキテクチャ内のサウスバウンドAPIはどのコンポーネントと通信しますか？

- A. ネットワーク内のコントローラー
- B. アプリケーション
- C. アプライアンス
- D. ルーターやスイッチなどのデバイス

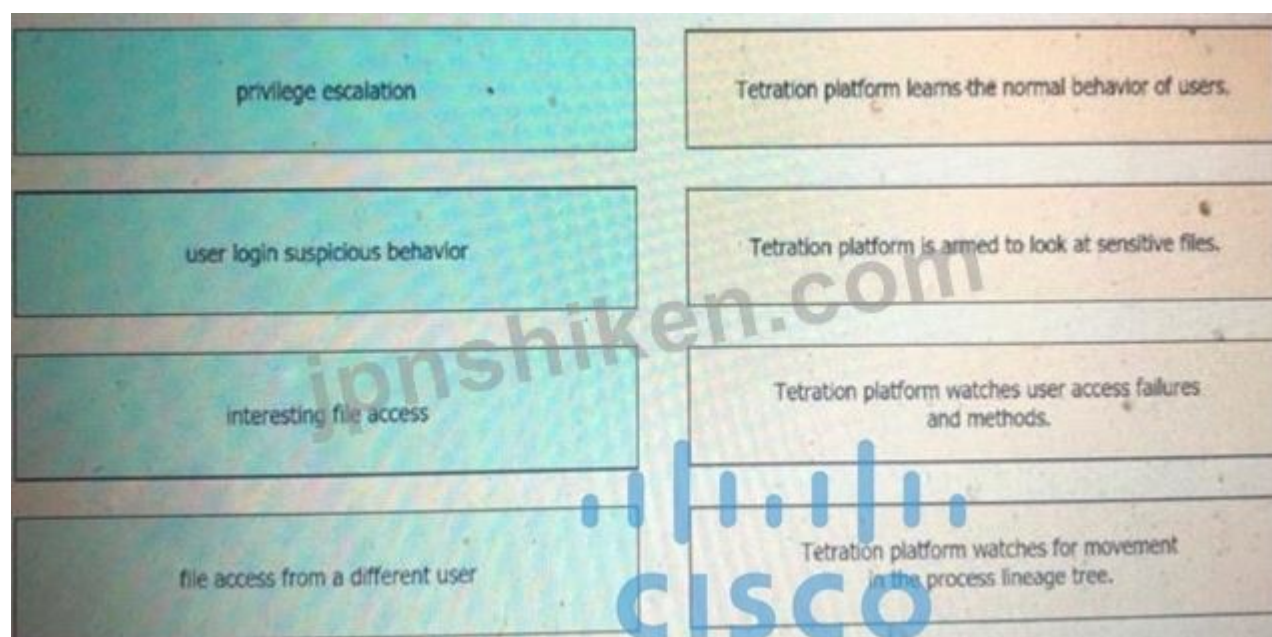
正解: ([正解を表示します](#))



サウスバウンドAPIは、コントローラーとネットワークデバイス間の通信に使用されます。

質問: 417

Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。



The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:

- **Shell code execution:** Looks for the patterns used by shell code.
- **Privilege escalation:** Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
- **Side channel attacks:** Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these
- **Raw socket creation:** Creation of a raw socket by a nonstandard process (for example, ping).
- **User login suspicious behavior:** Cisco Tetration platform watches user login failures and user login methods.
- **Interesting file access:** Cisco Tetration platform can be armed to look at sensitive files.
- **File access from a different user:** Cisco Tetration platform learns the normal behavior of which file is accessed by which
- **Unseen command:** Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command. Command lineage triggers the interest of the Tetration Analytics platform. (See Figure 10.)

正解:



<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html>

質問: 418

ネットワーク管理者は、ネットワーク上に現在存在する資産を確認する必要があります。サードパーティシステムは、ホストデータをCiscoFirepowerにフィードする必要があります。これを実現するには何を構成する必要がありますか？

A. ホストからデータを受信するためのネットワーク検出ポリシー

- B. ホストからデータをダウンロードするための脅威インテリジェンスポリシー
- C. ファイルデータをCiscoFirepowerに送信するためのファイル分析ポリシー
- D. ホストからNetFlowデータを受信するためのネットワーク分析ポリシー

正解: ([正解を表示します](#))

説明

説明

検出ルールを構成して、ホストおよびアプリケーションデータの検出をニーズに合わせて調整できます。

Firepowerシステムは、NetFlowエクスポーターからのデータを使用して、接続および検出イベントを生成し、ホストおよびアプリケーションデータをネットワークマップに追加できます。

ネットワーク分析ポリシーは、トラフィックのデコードと前処理の方法を管理するため、特に侵入の試みを示す可能性のある異常なトラフィックの場合は、さらに評価できます-回答Dは正しくありません。

質問: 419

Cisco FMCが、他の製品からセンサーに監視可能なセキュリティインテリジェンスをプッシュできるようにする製品はどれですか。

- A. 暗号化されたトラフィック分析
- B. Cisco Talos Intelligence
- C. 脅威インテリジェンスディレクター
- D. コグニティブ脅威分析

正解: C ([コメントを發表する](#))

質問: 420

組織のDMZには2つのシステムがあり、通信のためにそれらの間に暗号化されていないリンクがあります。

組織には定義済みのパスワードポリシーがなく、システムでいくつかのデフォルトアカウントを使用しています。

これらのシステムで使用されているアプリケーションも、厳格なコードレビューを受けていません。攻撃者がブルートフォースでシステムに侵入するのに役立つ脆弱性はどれですか？

- A. 弱いパスワード
- B. 入力検証の欠如
- C. 暗号化がありません
- D. ファイル権限の欠如

正解: ([正解を表示します](#))

質問: 421

DuoSecurityが組織に提供するような多要素認証ソリューションを実装する2つの理由は何ですか？ 2つ選択してください)

- A. 電話のコールバック、SMSパスコード、プッシュ通知など、2FAのさまざまな方法の柔軟性
- B. オンプレミスおよびクラウドアプリケーションへのシングルサインオンアクセス
- C. ネイティブのMicrosoftWindowsサブリカントを使用した802.1xセキュリティとの統合
- D. オンプレミスおよびクラウドアプリケーションへの安全なアクセス
- E. リソースへのアクセスを許可する前のアプリケーションの脆弱性の特定と修正

正解: ([正解を表示します](#))

二要素認証は、オンラインアカウントにセキュリティの第2層を追加します。2番目の要素（電話やその他のモバイルデバイスなど）を使用して本人確認を行うと、パスワードを知っている場合でも、自分以外の人にはログインできなくなります。

注：シングルサインオン（SSO）は、IDおよびアクセス管理のプロパティであり、ユーザーは1セットの資格情報（ユーザー名とパスワード）で1回だけログインすることにより、複数のアプリケーションとWebサイトで安全に認証できます。SSOを使用すると、ユーザーがアクセスしようとしているアプリケーションまたはWebサイトは、信頼できるサードパーティに依存して、ユーザーが本人であることを確認します。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード：**JPNshiken**」

質問: **422**

組織は、クラウド内のユーザー、データ、およびアプリケーションを保護したいと考えています。ソリューションはAPIベースであり、クラウドネイティブCASBとして動作する必要があります。この実装にはどのソリューションを使用する必要がありますか？

- A. Cisco Cloudlock
- B. Cisco Cloud Email Security
- C. Cisco Firepower次世代ファイアウォール
- D. Cisco Umbrella

正解: ([正解を表示します](#))

Cisco Cloudlock :クラウドネイティブのクラウドアクセスセキュリティブローカー（CASB）とクラウドサイバーセキュリティプラットフォームを使用して、クラウドユーザー、データ、およびアプリケーションを保護します。

Cisco Cloudlock :クラウドネイティブのクラウドアクセスセキュリティブローカー（CASB）とクラウドサイバーセキュリティプラットフォームを使用して、クラウドユーザー、データ、およびアプリケーションを保護します。

参照：

738565.pdf

Cisco Cloudlock :クラウドネイティブのクラウドアクセスセキュリティブローカー（CASB）とクラウドサイバーセキュリティプラットフォームを使用して、クラウドユーザー、データ、およびアプリケーションを保護します。

738565.pdf

質問: **423**

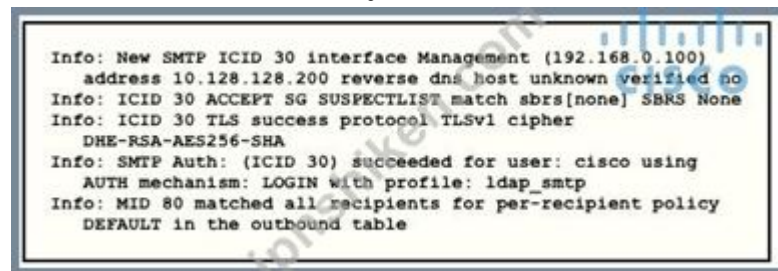
NetFlowがインターフェイスに適用される場合、設定されたレコードのキーフィールドと非キーフィールドに基づいてトラフィックを収集するために使用されるフローモニタキャッシュを作成するコンポーネントはどれですか。

- A. フローエクスポーター
- B. 記録
- C. フローサンプラー
- D. フローモニター

正解: **A** ([コメントを發表する](#))

質問: **424**

展示を参照してください。



どのタイプの認証が使用されていますか？

- A. SMTPリレーサーバー認証
- B. MicrosoftOutlookのLDAP認証
- C. POP3認証
- D. 外部ユーザーとリレーメール認証

正解: ([正解を表示します](#))

質問: 425

DoS攻撃とDDoS攻撃の違いは何ですか？

- A. DoS攻撃は、コンピューターを使用してサーバーをTCPパケットでフラッディングする場所ですが、DDoS攻撃は、コンピューターを使用してサーバーをUDPパケットでフラッディングする場所です。
- B. DoS攻撃は、コンピューターを使用してサーバーをTCPおよびUDPパケットでフラッディングする場所ですが、DDoS攻撃は、コンピューターを使用して、LAN上に分散されている複数のサーバーをフラッディングする場所です。
- C. DoS攻撃は、コンピューターを使用してサーバーをTCPパケットとUDPパケットで溢れさせる攻撃ですが、DDoS攻撃は、複数のシステムがDoS攻撃で単一のシステムを標的にする攻撃です。
- D. DoS攻撃は、コンピューターを使用してサーバーをUDPパケットでフラッディングする場所ですが、DDoS攻撃は、コンピューターを使用してサーバーをTCPパケットでフラッディングする場所です。

正解: ([正解を表示します](#))

質問: 426

Cisco Stealthwatch Cloudはどのようにクラウド環境にセキュリティを提供しますか？

- A. 敏感なdataの流出を防ぎます。
- B. 可視性と脅威の検出を提供します。
- C. パブリックネットワークとプライベートネットワーク間の安全な接続を容易にします。
- D. クライアントとサーバーにインターネットベースのDNS保護を割り当てます。

正解: B ([コメントを發表する](#))

質問: 427

ネットワーク上のトラフィックストームが原因で、2つのインターフェイスがエラー無効になり、両方のインターフェイスがSNMPトラップを送信しました。インターフェイスを確実にサービスに戻すには、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. Cisco Prime InfrastructureにSNMPsetコマンドを発行させて、事前設定された間隔の後にポートを再度有効にします。
- B. インターフェイスでshutdownコマンドとnoshutdownコマンドを入力します。
- C. EEMを使用して、ポートを300秒以内に自動的にサービスに戻します。

D. snmp-server enable trapsコマンドを有効にして、300秒待ちます

E. インターフェイスがエラー無効化の検出および回復機能で構成されていることを確認します。次のコマンドを使用してポートを起動することもできます。

+ shutdown」インターフェース構成コマンドの後に fioshutdown」インターフェース構成コマンドが続くと、無効になっているポートが再起動します。

+ errdisablerecoverycause...」グローバル構成コマンドは、タイマーがエラー無効状態を自動的に回復できるようにし、

errdisablerecoveryintervalinterval」グローバル構成コマンドはエラー無効状態を回復する時間を指定します。

正解: ([正解を表示します](#))

質問: 428

CiscoSecurityIntelligenceがCiscoNextGeneration Intrusion Prevention Systemで機能するには、どのライセンスが必要ですか。

A. コントロール

B. 保護する

C. URLフィルタリング

D. マットウェア

正解: ([正解を表示します](#))

質問: 429

URLが悪意があるかどうかを判断するためにCiscoUmbrellaを統合するCiscoソリューションはどれですか。

A. タロス

B. DynDNS

C. AnyConnect

D. AMP

正解: ([正解を表示します](#))

質問: 430

どのアルゴリズムが非対称暗号化を提供しますか？

A. RC4

B. RSA

C. AES

D. 3DES

正解: B ([コメントを发表する](#))

<https://securityboulevard.com/2020/05/types-of-encryption-5-encryption-algorithms-how-to-choose-the-right-one/#:~:text=Standard%20asymmetric%20encryption%20algorithms%20include,%2C%20El%20Gamal%2C%20and%20DSA。>

質問: 431

CiscoASA用のCiscoNetFlowセキュアイベントロギングの機能は何ですか。

A. 複数のNetFlowコレクターがサポートされています

B. 高度なNetFlowv9テンプレートとレガシーv5フォーマットがサポートされています

C. セキュアNetFlow接続はCiscoPrimeInfrastructure用に最適化されています

D. フロー作成イベントが遅延します

正解: ([正解を表示します](#))

説明説明NetFlowセキュアイベントロギング (NSEL) のASAおよびASASM実装は、次の主要な機能を提供します。...-フロー作成イベントのエクスポートを遅延させます。参照 <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.pdf>説明ASAおよびASASMの実装NetFlowセキュアイベントロギング (NSEL) は、次の主要な機能を提供します。

..。

-フロー作成イベントのエクスポートを遅らせます。

説明説明NetFlowセキュアイベントロギング (NSEL) のASAおよびASASM実装は、次の主要な機能を提供します。...-フロー作成イベントのエクスポートを遅延させます。参照 <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.pdf>

質問: **432**

組織は、インフラストラクチャに新しいファイアウォールを追加する必要があり、CiscoASAまたはCiscoFTDを使用したいと考えています。選択したファイアウォールは、警告ページを表示した後に特定のサイトのブロックをバイパスし、接続をリセットするオプションをユーザーに提供するなど、トラフィックをブロックする方法を提供する必要があります。組織はどのソリューションを選択する必要がありますか？

A. Cisco FTDは、システムレートレベルのトラフィックブロッキングをサポートしているのに対し、CiscoASAはサポートしていないため

B. Cisco FTDは、インタラクティブなブロッキングとリセットによるブロッキングをネイティブに有効にしますが、CiscoASAは有効にしません。

C. Cisco ASAは、インタラクティブブロッキングおよびリセット付きブロッキングをGUIを介して設定できるためですが、CiscoFTDでは設定できません。

D. Cisco ASAには、複数のブロッキング機能を提供するためにインストールできる追加のモジュールがありますが、CiscoFTDにはありません。

正解: ([正解を表示します](#))

質問: **433**

IPsecで使用する2つの暗号化アルゴリズムはどれですか？{2つ選択してください。}

- A.** AES-BAC
- B.** AES-ABC
- C.** HMAC-SHA1 / SHA2
- D.** トリプルAMC-CBC
- E.** AES-CBC

正解: **C,E** ([コメントを发表する](#))

説明

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ips

質問: **434**

展示を参照してください。

```

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C   1.1.1.0 255.255.255.0 is directly connect, outside
S   172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C   192.168.100.0 255.255.255.0 is directly connected, inside
C   172.16.10.0 255.255.255.0 is directly connected, dmz
S   10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
match access-list redirect-acl

policy-map inside-policy
class redirect-class
sfr fail-open

service-policy inside-policy global

```

構成の結果は何ですか？

- A. DMZネットワークからのトラフィックがリダイレクトされます
- B. 内部ネットワークからのトラフィックはリダイレクトされます
- C. すべてのTCPトラフィックがリダイレクトされます
- D. 内部およびDMZネットワークからのトラフィックがリダイレクトされます

正解: (正解を表示します)

上記のコマンドの目的は、ACL `redirect-acl` に一致するトラフィックをインライン（通常モードのCisco FirePOWER SFR）モジュールにリダイレクトすることです。このモードでは、不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはASAに戻され、さらに処理され、最終的に送信されます。コマンド `service-policy global_policy global` は、ポリシーをすべてのインターフェースに適用します。参照 <https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html> インライン（通常モードのFirePOWER SFR）モジュール。このモードでは、不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはASAに戻され、さらに処理され、最終的に送信されます。

コマンド `service-policy global_policy global` は、ポリシーをすべてのインターフェースに適用します。

上記のコマンドの目的は、ACL `redirect-acl` に一致するトラフィックをインライン（通常モードのCisco FirePOWER SFR）モジュールにリダイレクトすることです。このモードでは、不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはASAに戻され、さらに処理され、最終的に送信されます。コマンド `service-policy global_policy global` は、ポリシーをすべてのインターフェースに適用します。参照 <https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html>

質問: 435

組織は、クラウド内のユーザー、データ、およびアプリケーションを保護したいと考えています。ソリューションはAPIベースであり、クラウドネイティブのCAS8として動作する必要があります。この実装には多くのソリューションを使用する必要がありますか？

- A. Cisco Cloudlock
- B. CiscoFirepower次世代ファイアウォール
- C. Cisco Cloud Email Security
- D. Cisco Umbrella

正解: **A** ([コメントを发表する](#))

質問: **436**

どの姿勢評価要件がクライアントに修復のオプションを提供し、特定の時間枠内の修復を必要としますか？

- A. 監査
- B. 必須
- C. オプション
- D. 可視性

正解: ([正解を表示します](#))

ポスチャ要件は、役割およびオペレーティングシステムにリンクできる、関連する修復アクションを伴う一連の複合条件です。ネットワークに接続するすべてのクライアントは、ネットワークに準拠するために、姿勢評価中に必須の要件を満たす必要があります。ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。要件がオプションであり、クライアントがこれらの要件を満たしていない場合、クライアントはエンドポイントのポスチャ評価中に続行するオプションがあります。必須要件ポリシーの評価中に、エージェントは、ポスチャポリシーで定義された必須要件を満たしていないクライアントに修復オプションを提供します。エンドユーザーは、修復タイマー設定で指定された時間内に要件を満たすために修復する必要があります。例えば、絶対パスにC \ temp \ text.fileが存在することを確認するために、ユーザー定義の条件で必須要件を指定しました。ファイルが存在しない場合、必須要件は失敗し、ユーザーは非準拠状態に移行します。参照：

https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.htmlポスチャポリシー要件は、必須、オプション、またはポスチャポリシーの監査タイプ。要件がオプションであり、クライアントがこれらの要件を満たしていない場合、クライアントはエンドポイントのポスチャ評価中に続行するオプションがあります。必須要件は失敗し、ユーザーは非準拠状態に移行します。参照 https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.htmlポスチャポリシー要件は、必須、オプション、またはポスチャポリシーの監査タイプ。要件がオプションであり、クライアントがこれらの要件を満たしていない場合、クライアントはエンドポイントのポスチャ評価中に続行するオプションがあります。必須要件は失敗し、ユーザーは非準拠状態に移行します。参照 https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.htmlポスチャポリシー要件は、必須、オプション、またはポスチャポリシーの監査タイプ。要件がオプションであり、クライアントがこれらの要件を満たしていない場合、クライアントはエンドポイントのポスチャ評価中に続行するオプションがあります。

必須要件

ポリシーの評価中に、エージェントは、ポスチャポリシーで定義された必須要件を満たしていないクライアントに修復オプションを提供します。エンドユーザーは、修復タイマー設定で指定された時間内に要件を満たすために修復する必要があります。

たとえば、絶対パスにC \ temp \ text.fileが存在することを確認するために、ユーザー定義の条件で必須要件を指定しました。ファイルが存在しない場合、必須要件は失敗し、ユーザーは非準拠状態に移行します。

参照：

ポスチャ要件は、役割およびオペレーティングシステムにリンクできる、関連する修復アクションを伴う一連の複合条件です。ネットワークに接続するすべてのクライアントは、ネットワークに準拠するために、姿勢評価中に必須の要件を満たす必要があります。ポスチャポリシー要件は、ポスチャポリシーで必須、オプション、または監査タイプに設定できます。要件がオプションであり、クライアントがこれらの要件を満たしていない場合、クライアントはエンドポイントのポスチャ評価中に続行するオプションがあります。必須要件ポリシーの評価中に、エージェントは、ポスチャポリシーで定義された必須要件を満たしていないクライアントに修復オプションを提供します。エンドユーザーは、修復タイマー設定で指定された時間内に要件を満たすために修復する必要があります。

すために修復する必要があります。例えば、絶対パスにC \ temp \ text.fileが存在することを確認するために、ユーザー定義の条件で必須要件を指定しました。ファイルが存在しない場合、必須要件は失敗し、ユーザーは非準拠状態に移行します。参照：

https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.html

有効的な**350-701**問題集はJPNTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTest.comは今最新**350-701**試験問題集を提供します。JPNTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **437**

NetFlowフローモニタリングの2つの機能は何ですか？ 2つ選択してください)

- A. 入力および出力情報を追跡できます
- B. フローレコードとフローインポーターを含める
- C. すべての入力フロー情報をインターフェイスにコピーします
- D. インターフェイスでのパケットサンプリングは必要ありません
- E. マルチキャスト、MPLS、またはブリッジトラフィックの追跡に使用できます

正解: ([正解を表示します](#))

説明FlexibleNetFlowの制限事項は次のとおりです。+従来のNetFlow (NF) アカウンティングはサポートされていません。+フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。+入力と出力の両方のNetFlowアカウンティングがサポートされています。+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。+インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。参照：

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/solidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html

NetFlowを設定するときは、次のガイドラインと制限に従ってください。+PFC3Aモードを除く、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。+NetFlowはマルチキャストIPトラフィックをサポートします。参照：
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.htmlフレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルーターに到着するパケットのIPフロー情報をマルチプロトコルラベルスイッチング (MPLS) パケットとしてキャプチャできます。IPパケットとして送信されます。この機能を使用すると、サービスプロバイダバックボーンを介してVPNのあるサイトから同じVPNの別のサイトに移動するMPLS VPN IPフローをキャプチャできます。<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html>以下はFlexibleNetFlowの制限事項です。htmlフレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、サービスプロバイダバックボーンを介してVPNのあるサイトから同じVPNの別のサイトに移動するMPLS VPN IPフローをキャプチャできます。<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html>以下はFlexibleNetFlowの制限事項です。htmlフレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、サービスプロバイダバックボーンを介してVPNのあるサイトから同じVPNの別のサイトに移動するMPLS VPN IPフローをキャプチャできます。<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html>以下はFlexibleNetFlowの制限事項です。

+従来のNetFlow (NF) アカウンティングはサポートされていません。

+フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。

+入力と出力の両方のNetFlowアカウンティングがサポートされています。
+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。
+インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。
参照：

Consolidated_guide / b_consolidated_3850_3se_cg_chapter_011010.html

NetFlowを設定するときは、次のガイドラインと制限に従ってください。

+ PFC3Aモードを除いて、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。

+NetFlowはマルチキャストIPトラフィックをサポートします。

フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、ルータにマルチプロトコルラベルスイッチング (MPLS) パケットとして到着し、IPパケットとして送信されるパケットのIPフロー情報をキャプチャできます。この機能を使用すると、サービスプロバイダーバックボーンを介してVPNのあるサイトから同じVPNの別のサイトに移動するMPLS VPN IPフローをキャプチャできます。説明以下は、FlexibleNetFlowの制限事項です。+従来のNetFlow (TNF) アカウンティングはサポートされています。+フレキシブルNetFlowv5エクスポート形式はサポートされていません。NetFlowv9エクスポート形式のみがサポートされています。+入力と出力の両方のNetFlowアカウンティングがサポートされています。+ Microflowポリシング機能は、NetFlowハードウェアリソースをFNFと共有します。+インターフェイスごとおよび方向ごとに1つのフローモニターのみがサポートされます。参照：

[https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/Consolidated_guide/](https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/Consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html)

[b_consolidated_3850_3se_cg_chapter_011010.html](https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/Consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html) NetFlowを設定するときは、次のガイドラインと制限に従ってください。+ PFC3Aモードを除き、NetFlowはブリッジIPトラフィックをサポートします。PFC3Aモードは、NetFlowブリッジIPトラフィックをサポートしていません。+NetFlowはマルチキャストIPトラフィックをサポートします。参照 https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html フレキシブルNetFlow-MPLS出力NetFlow機能を使用すると、マルチプロトコルラベルスイッチング (MPLS) パケットとしてルーターを使用し、IPパケットとして送信されます。この機能を使用すると、VPNのあるサイトから同じVPNリファレンスの別のサイト (<https://www.cisco.com>) にサービスプロバイダーバックボーンを通過するMPLSVPNIPフローをキャプチャできます。

質問: 438

CiscoDNACenterで使用されるIntegrationAPIの2つの機能はどれですか。2つ選択してください)

- A. 無線LANコントローラで新しいSSIDを作成する
- B. 新しい仮想ルーターを自動的に展開します。
- C. スイッチとルーターのソフトウェアをアップグレードします。
- D. デバイスおよびIoTセンサーの電力使用率を監視するアプリケーション。
- E. 情報技術サービス管理プラットフォームに接続する

正解: A,B ([コメントを发表する](#))

質問: 439

ネットワーク管理者が新しいルーターでSNMPv3を構成しています。ユーザーはすでに作成されています。ただし、SNMPビューへのアクセスを容易にするために、追加の構成が必要です。これを達成するために管理者は何をしなければなりませんか？

- A. SNMPv3ユーザーをSNMPビューにマップします
- B. SNMPが使用するUDPポートを指定します
- C. SNMPv3認証に使用するパスワードを設定します
- D. SNMPv3で使用する暗号化アルゴリズムを定義します

正解: ([正解を表示します](#))

質問: **440**

展示を参照してください。Pythonスクリプトの結果は何ですか？

- A. POST HTTPメソッドを使用して、認証に使用されるトークンを取得します。
- B. GET HTTPメソッドを使用して、認証に使用されるトークンを取得します。
- C. GET HTTPメソッドを使用して、認証に使用するユーザー名とパスワードを取得します
- D. POST HTTPメソッドを使用して、認証に使用するユーザー名とパスワードを取得します。

正解: **A** ([コメントを發表する](#))

質問: **441**

エンジニアがCiscoESAを設定していて、受信者アドレスへの電子メールメッセージを受け入れるか拒否するかを制御したいと考えています。許可された受信者アドレスが含まれているリストはどれですか？

- A. BAT
- B. SAT
- C. RAT
- D. HAT

正解: ([正解を表示します](#))

質問: **442**

SDNアーキテクチャのノースバウンドAPIの主な機能は、ネットワークのどの2つの領域間の通信を可能にすることです。

- A. SDNコントローラーとクラウド
- B. 管理コンソールとSDNコントローラー
- C. SDNコントローラーと管理ソリューション
- D. 管理コンソールとクラウド

正解: ([正解を表示します](#))

質問: **443**

XSS攻撃とSQLインジェクション攻撃の違いは何ですか？

- A. SQLインジェクションはSQLデータベースを攻撃するために使用されるハッキング方法ですが、XSS攻撃はさまざまな種類のアプリケーションに存在する可能性があります
- B. XSSはSQLデータベースを攻撃するために使用されるハッキング方法ですが、SQLインジェクション攻撃はさまざまな種類のアプリケーションに存在する可能性があります
- C. SQLインジェクション攻撃はデータベースから情報を盗むために使用されますが、XSS攻撃は、攻撃者がデータベースからデータを盗むことができるWebサイトにユーザーをリダイレクトするために使用されます
- D. XSS攻撃はデータベースから情報を盗むために使用されますが、SQLインジェクション攻撃は、攻撃者がデータを盗むことができるWebサイトにユーザーをリダイレクトするために使用されます

正解: ([正解を表示します](#))

XSSでは、攻撃者は自分の悪意のあるコード（通常は悪意のあるリンク）をデータベースに挿入しようとします。他のユーザーが彼のリンクをたどると、彼らのWebブラウザは、攻撃者がそれらからデータを盗むことができるWebサイトにリダイレクトされます。SQLインジェクションでは、攻撃者は

ブラウザを介して)SQLコードを、GET / POSTパラメータのデータサニタイズまたは検証メソッドを使用しないフォーム、Cookie、またはHTTPヘッダーに挿入しようとします。

質問: 444

DuoSecurityが組織に提供するような多要素認証ソリューションを実装する2つの理由は何ですか？ 2つ選択してください。)

- A. オンプレミスおよびクラウドアプリケーションへの安全なアクセス
- B. 電話コールバック、SMSパスコードなどの2FAのさまざまな方法の柔軟性。とプッシュ通知
- C. リソースへのアクセスを許可する前のアプリケーションの脆弱性の特定と修正
- D. オンプレミスおよびクラウドアプリケーションへのシングルサインオンアクセス
- E. ネイティブのMicrosoftWindowsサブリカントを使用した802.1xセキュリティとの統合

正解: ([正解を表示します](#))

質問: 445

オンプレミスではない環境での侵害、アプリケーションリスク、およびデータ侵害を削減するのに役立つCiscoAPIベースのブローカとは何ですか。

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco AMP
- D. Cisco App Dynamics

正解: A ([コメントを發表する](#))

参照 :

Cisco Cloudlock is the API-based cloud access security broker (CASB) that helps accelerate use of the cloud. By securing your identities, data, and apps, Cloudlock combats account compromises, breaches, and cloud app ecosystem risks. Our API-driven approach provides a simple and open way to enable healthy cloud adoption.

質問: 446

CiscoIOSデバイスで許可状態が正常に変更された場合に送信されるCoA応答コードはどれですか。

- A. CoA-ACK
- B. CoA-NCL
- C. COA-MAB
- D. CoA-NAK

正解: ([正解を表示します](#))

質問: 447

エンジニアは、pxGridを使用してCiscoFMCとCiscoISEを統合します。CiscoFMCに割り当てられている役割はどれですか。

- A. サーバー
- B. コントローラー
- C. クライアント
- D. 発行元

正解: ([正解を表示します](#))

質問: 448

Cisco ASAは、暗号化されたCiscoUnifiedCommunicationsトラフィックのTLSプロキシをサポートする必要があります。

Cisco UC ManagerプラットフォームのどこにASAを追加する必要がありますか？

- A. 証明書の信頼リスト
- B. エンドポイント信頼リスト
- C. エンタープライズプロキシサービス
- D. セキュリティで保護されたコラボレーションプロキシ

正解: A ([コメントを發表する](#))

説明/リファレンス <https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html>

質問: 449

管理者は、CiscoIOSルータで新しいサイト間VPN接続を確立しています。組織は、ハブのISAKMPキーが、のIPアドレスからのトラフィックを終了するためにのみ使用されるようにする必要があります。

172.19.20.24。管理者がこれを実行できるようにするハブのコマンドはどれですか？

- A. 暗号通貨ID 172.19.20.24
- B. 暗号isakmpキーCisco0123456789 172.19.20.24
- C. 暗号登録ピアアドレス172.19.20.24
- D. cryptoisakmpIDアドレス172.19.20.24

正解: B ([コメントを發表する](#))

コマンド `cryptoisakmpidentityaddress172.19.20.24`は無効です。 `cryptoisakmpidentity{address | hostname}`のみを使用できます。次の例では、2つのピアで事前共有キーを使用し、両方のISAKMPIDをIPアドレスに設定します。

ローカルピア (10.0.0.1)で、ISAKMP IDが設定され、事前共有キーが指定されます。

cryptoisakmpIDアドレス

`crypto isakmp key sharedkeystring address 192.168.1.33`

リモートピア (192.168.1.33)で、ISAKMP IDが設定され、同じ事前共有キーが指定されます。

cryptoisakmpIDアドレス

`crypto isakmp key sharedkeystring address 10.0.0.1`

コマンド `cryptoisakmpidentityaddress172.19.20.24`は無効です。 `cryptoisakmpidentity{address | hostname}`のみを使用できます。次の例では、2つのピアで事前共有キーを使用し、両方のISAKMPIDをIPアドレスに設定します。

ローカルピア (10.0.0.1)で、ISAKMP IDが設定され、事前共有キーが指定されます。

cryptoisakmpIDアドレス

`crypto isakmp key sharedkeystring address 192.168.1.33`

リモートピア (192.168.1.33)で、ISAKMP IDが設定され、同じ事前共有キーが指定されます。

cryptoisakmpIDアドレス

`crypto isakmp key sharedkeystring address 10.0.0.1`

参照：

コマンド `cryptoenrollmentpeeraddress`も無効です。

コマンド `cryptocaidentity...`は、ルータの信頼できるCAを宣言するためにのみ使用され、caidentityコンフィギュレーションモードになります。また、その後IPアドレスではなく名前を付ける必要があります。例：`cryptocaidentityCA-Server`]->回答Aは正しくありません。

答えBだけが残っている最良の選択です。

コマンド `cryptoisakmpidentityaddress172.19.20.24`は無効です。 `cryptoisakmpidentity{address | hostname}`のみを使用できます。次の例では、2つのピアで事前共有キーを使用し、両方のISAKMPIDをIPアドレスに設定します。

ローカルピア (10.0.0.1)で、ISAKMP IDが設定され、事前共有キーが指定されます。

cryptoisakmpIDアドレス

crypto isakmp key sharedkeystring address 192.168.1.33

リモートピア (192.168.1.33)で、ISAKMP IDが設定され、同じ事前共有キーが指定されます。

cryptoisakmpIDアドレス

crypto isakmp key sharedkeystring address 10.0.0.1

コマンド `cryptoenrollmentpeeraddress`も無効です。

コマンド `cryptocaidentity...`は、ルータの信頼できるCAを宣言するためにのみ使用され、caidentityコンフィギュレーションモードになります。また、その後IPアドレスではなく名前を付ける必要があります。例：`cryptocaidentityCA-Server`]->回答Aは正しくありません。

コマンド `cryptoenrollmentpeeraddress`も無効です。

コマンド `cryptocaidentity...`は、ルータの信頼できるCAを宣言するためにのみ使用され、caidentityコンフィギュレーションモードになります。また、その後IPアドレスではなく名前を付ける必要があります。例：`cryptocaidentityCA-Server`]->回答Aは正しくありません。

答えBだけが残っている最良の選択です。

質問: 450

Cisco ESA管理者は、隔離された電子メールが配信される前にウイルスがないことを確認するようにCiscoESAを設定する必要があります。さらに、既知の不良メールサーバーからのメールの配信を防止する必要があります。これらの要件を満たすために実行する必要がある2つのアクションはどれですか？ 2つ選択してください)

- A. SenderBaseのアウトブレイクフィルターを使用する
- B. メッセージ追跡サービスを有効にする
- C. 受信者アクセステーブルを設定します
- D. CiscoESAをDMZに導入します
- E. アンチウイルス署名を使用して隔離された電子メールをスキャンする

正解: ([正解を表示します](#))

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせ

ずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。

SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

参照 :

b_ESA_Admin_Guide_12_0 / b_ESA_Admin_Guide_12_0_chapter_0100100.html

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

注 :リモートアクセストロイの木馬 (RAT)と混同しないように、受信者アクセステーブル (RAT)は、パブリックリスナーが受け入れる受信者を定義するCiscoESA用語です。

b_ESA_Admin_Guide_12_0 / b_ESA_Admin_Guide_12_0_chapter_0100100.html

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

b_ESA_Admin_Guide_12_0 / b_ESA_Admin_Guide_12_0_chapter_0100100.html

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

注 :リモートアクセストロイの木馬 (RAT)と混同しないように、受信者アクセステーブル (RAT)は、パブリックリスナーが受け入れる受信者を定義するCiscoESA用語です。

質問: 451

ソフトウェア定義のネットワークアーキテクチャ内のコントローラーがネットワーク内のスイッチの構成を動的に変更する場合、どのタイプのAPIが使用されますか？

A. イーストバウンドAPI

B. 西行きAP

C. サウスバウンドAPI

D. ノースバウンドAPI

正解: ([正解を表示します](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 452

CiscoESAでは防止できるがCiscoWSAでは防止できない攻撃はどれですか。

- A. バッファオーバーフロー
- B. DoS
- C. SQLインジェクション
- D. フィッシング

正解: **D** ([コメントを发表する](#))

Cisco EmailSecurityGatewayにCiscoAdvancedPhishingProtectionを導入する利点は次のとおりです。以下を防止します。+侵害されたアカウントとソーシャルエンジニアリングを使用する攻撃。+フィッシング、ランサムウェア、ゼロデイ攻撃、なりすまし。+悪意のあるペイロードまたはURLのないBEC。
参照 https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.htmlゲートウェイ:

次のことを防ぎます。

- +侵害されたアカウントとソーシャルエンジニアリングを使用する攻撃。
- +フィッシング、ランサムウェア、ゼロデイ攻撃、なりすまし。
- +悪意のあるペイロードまたはURLのないBEC。

参照:

Cisco EmailSecurityGatewayにCiscoAdvancedPhishingProtectionを導入する利点は次のとおりです。以下を防止します。+侵害されたアカウントとソーシャルエンジニアリングを使用する攻撃。+フィッシング、ランサムウェア、ゼロデイ攻撃、なりすまし。+悪意のあるペイロードまたはURLのないBEC。
参照 https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

質問: **453**

IaaSクラウドサービスモデルでは、プロバイダーが管理を担当するセキュリティ機能はどれですか？

- A. インターネットプロキシ
- B. 仮想マシンのファイアウォール
- C. CASB
- D. ハイパーバイザーOSの強化

正解: **B** ([コメントを发表する](#))

このIaaSモデルでは、クラウドプロバイダーは、仮想マシンとしてのコンピューター、raw (ブロック)ストレージ、ファイアウォール、ロードバランサー、およびネットワークデバイスを含むユーザー/マシンにリソースを提供します。

注:クラウドアクセスセキュリティブローカー (CASB)は、可視性とコンプライアンスチェックを提供し、データを誤用や漏洩から保護し、ランサムウェアなどのマルウェアに対する脅威から保護します。

質問: **454**

CiscoDNACenterで使用するIntegrationAPIの2つの機能はどれですか。(2つ選択してください)

- A. 新しい仮想ルーターを自動的に展開する
- B. スイッチとルーターのソフトウェアをアップグレードする
- C. デバイスとIoTセンサーの電力使用率を監視するアプリケーション
- D. 情報技術サービス管理プラットフォームに接続する
- E. 無線LANコントローラで新しいSSIDを作成する

正解: ([正解を表示します](#))

Integration API (Westbound) 統合機能はWestboundインターフェースの一部です。最新のデータセンターでの運用を拡張および加速する必要性を満たすために、ITオペレーターは、オープンAPIで構築されたインテリジェントなエンドツーエンドのワークフローを必要としています。Cisco DNA Centerプラットフォームは、Cisco DNA AssuranceワークフローとデータをサードパーティのITサービス管理 (ITSM) ソリューションと統合するためのメカニズムを提供します。参照: <https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/events-andnotifications-eastbound>。したがって、回答Dは正しいです。Westbound-統合API Cisco DNA Centerプラットフォームは、ITSM、IPAM、レポートなどのさまざまなドメインを統合することにより、バリューチェーン全体でエンドツーエンドのITプロセスを強化できます。RESTベースの統合アダプターAPIを活用することにより、双方向インターフェイスを構築して、Cisco DNA Centerと外部のサードパーティITシステムとの間でコンテキスト情報を交換できるようにすることができます。Westbound APIは、ネットワークデータ、イベント、および通知を外部システムに公開し、接続されたシステムからCisco DNA Centerの情報を消費する機能を提供します。参照: <https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage>。したがって、最も適切な選択は、統合APIがデバイスとIoTセンサーの電力使用率を監視できることです。イベントと外部システムへの通知を行い、接続されたシステムからCisco DNA Centerの情報を消費します。参照: <https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage>。したがって、最も適切な選択は、統合APIがデバイスとIoTセンサーの電力使用率を監視できることです。イベントと外部システムへの通知を行い、接続されたシステムからCisco DNA Centerの情報を消費します。参照:

<https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage>。したがって、最も適切な選択は、統合APIがデバイスとIoTセンサーの電力使用率を監視できることです。→回答Cは正解です。

統合機能はWestboundインターフェースの一部です。最新のデータセンターでの運用を拡張および加速する必要性を満たすために、ITオペレーターは、オープンAPIで構築されたインテリジェントなエンドツーエンドのワークフローを必要としています。Cisco DNA Centerプラットフォームは、Cisco DNA AssuranceワークフローとデータをサードパーティのITサービス管理 (ITSM) ソリューションと統合するためのメカニズムを提供します。

参照:

→したがって、回答Dは正解です。

Westbound-統合API

Cisco DNA Centerプラットフォームは、ITSM、IPAM、レポートなどのさまざまなドメインを統合することにより、バリューチェーン全体でエンドツーエンドのITプロセスを強化できます。RESTベースのIntegration Adapter APIを活用することにより、双方向インターフェイスを構築して、Cisco DNA Centerと外部のサードパーティITシステムとの間でコンテキスト情報を交換できるようになります。Westbound APIは、ネットワークデータ、イベント、および通知を外部システムに公開し、接続されたシステムからCisco DNA Centerの情報を消費する機能を提供します。したがって、最も適切な選択は、統合APIがデバイスの電力使用率を監視でき、IoT統合API (Westbound) 統合機能はWestboundインターフェースの一部であるということです。最新のデータセンターでの運用を拡張および加速する必要性を満たすために、ITオペレーターは、オープンAPIで構築されたインテリジェントなエンドツーエンドのワークフローを必要としています。Cisco DNA Centerプラットフォームは、Cisco DNA AssuranceワークフローとデータをサードパーティのITサービス管理 (ITSM) ソリューションと統合するためのメカニズムを提供します。参照:

<https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/events-andnotifications-eastbound>。したがって、回答Dは正しいです。Westbound-統合API Cisco DNA Centerプラットフォームは、ITSM、IPAM、レポートなどのさまざまなドメインを統合することにより、バリューチェーン全体でエンドツーエンドのITプロセスを強化できます。RESTベースのIntegration Adapter APIを活用することにより、双方向インターフェイスを構築して、Cisco DNA Centerと外部のサードパーティITシステムとの間でコンテキスト情報を交換できるようになります。Westbound APIは、ネットワークデータ、イベント、および通知を外部システムに公開し、接続されたシステムからCisco DNA Centerの情報を消費する機能を提供します。参照: <https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage>。したがって、最も適切な選択は、統合APIがデバイスとIoTセンサーの電力使用率を監視できることです。→回答Cは正解です。Westbound APIは、ネットワークデータ、イベント、および通知を外部システムに公開し、接続されたシステムからCisco DNA Centerの情報を消費する機能を提供します。参照:

<https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage>。したがって、最も適切な選択は、統合APIがデバイスとIoTセンサーの電力使用率を監視できることです。→回答Cは正解です。Westbound APIは、ネットワークデータ、イベント、および通知を外

部システムに公開し、接続されたシステムからCiscoDNACenterの情報を消費する機能を提供します。参照 <https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage>したがって、最も適切な選択は、統合APIがデバイスとIoTセンサーの電力使用率を監視できることです→回答Cは正解です。

質問: 455

企業は、オンプレミスに保存されていないクレジットカード番号の流出を経験しています。会社は、環境全体で機密データを保護できる必要があります。この目標を達成するには、どのツールを使用する必要がありますか？

- A. セキュリティマネージャー
- B. クラウドロック
- C. Webセキュリティアプライアンス
- D. Cisco ISE

正解: **B** ([コメントを發表する](#))

Cisco Cloudlockは、クラウドへの安全な移行を支援するクラウドネイティブのクラウドアクセスセキュリティブローカー (CASB)です。クラウドユーザー、データ、アプリを保護します。Cisco Cloudlockは、可視性とコンプライアンスチェックを提供し、データを誤用や流出から保護し、ランサムウェアなどのマルウェアに対する脅威から保護します。

質問: 456

電子メール管理者が新しいCiscoESAを設定しています。管理者は、のブロックを有効にしたいと考えていますエンドユーザー向けのgreymail。管理者が最初に有効にする必要がある機能はどれですか？

- A. アンチウイルスフィルタリング
- B. IPレピュテーションフィルタリング
- C. ファイル分析
- D. インテリジェントマルチスキャン

正解: ([正解を表示します](#))

質問: 457

crypto isakmp key ciscXXXXXXXXX address 172.16.0.0コマンドを実行した結果はどうなりますか？

- A. キーciscXXXXXXXXXを使用して、172.16.0.0/16の範囲のIKEv2ピアを認証します
- B. キーciscXXXXXXXXXを使用して、172.16.0.0/32ピアのIPアドレスを認証します
- C. キーciscXXXXXXXXXを使用して、172.16.0.0/16の範囲のIKEv1ピアを認証します
- D. キーciscXXXXXXXXXを使用して、IKEExchange内のすべての証明書を保護します

正解: **A** ([コメントを發表する](#))

上記のコマンドの構文は次のとおりです。

crypto isakmp key enc-type-digit keystore {address peer-address [mask] | ipv6 ipv6-address / ipv6-prefix | hostname hostname} [no-xauth] peer-address引数は、リモートピアのIPアドレスまたはIPv6アドレスを指定します。

上記のコマンドの構文は次のとおりです。

crypto isakmp key enc-type-digit keystore {address peer-address [mask] | ipv6 ipv6-address / ipv6-prefix | hostname hostname} [no-xauth] peer-address引数は、リモートピアのIPアドレスまたはIPv6アドレスを指定します。

参照：

上記のコマンドの構文は次のとおりです。

crypto isakmp key enc-type-digit keystring {address peer-address [mask] | ipv6 ipv6-address / ipv6-prefix | hostname hostname} [no-xauth] peer-address引数は、リモートピアのIPアドレスまたはIPv6アドレスを指定します。

質問: **458**

マルチベンダー環境をサポートし、サイト間のトラフィックを保護できるVPNテクノロジーはどれですか？

- A. SSL VPN
- B. VPNを取得
- C. FlexVPN
- D. DMVPN

正解: ([正解を表示します](#))

説明FlexVPNはIKEv2ベースのVPNテクノロジーであり、従来のサイト間VPN実装を超えるいくつかの利点を提供します。FlexVPNは、Cisco以外のIKEv2実装と相互運用できる標準ベースのソリューションです。したがって、FlexVPNはマルチベンダー環境をサポートできます。3つのVPNテクノロジーはすべて、サイト間のトラフィック サイト間またはスポークツースポーク)をサポートします。

質問: **459**

Cisco FMCが、他の製品からセンサーに監視可能なセキュリティインテリジェンスをプッシュできるようにする製品はどれですか。

- A. 暗号化されたトラフィック分析
- B. 脅威インテリジェンスディレクター
- C. コグニティブ脅威分析
- D. Cisco Talos Intelligence

正解: **B** ([コメントを发表する](#))

説明

As shown in the image, on the FMC you have to configure sources from where you would like to download threat intelligence information. The FMC then pushes that information (observables) to sensors. When the traffic matches the observables, the incidents appear in the FMC user interface (GUI).

<https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cis>

質問: **460**

展示を参照してください。

```

> show crypto ipsec sa
interface: Outside
  Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
  209.165.200.225

    access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
    255.255.255.0 10.0.10.0 255.255.255.0
    local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
    current_peer: 209.165.202.129

    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
    failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments
    created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
    reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
    209.165.202.129/500
    path mtu 1500, ipsec overhead 55(36), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: B6F5EA53
    current inbound spi : 84348DEE

```

トラフィックは、FirepowerThreatDefenseアプライアンスのIPsecサイト間VPNを通過していません。この問題の原因は何ですか？

- A. FirepowerThreatDefenseアプライアンスで分割トンネルポリシーが定義されていません。
- B. アクセス制御ポリシーはでVPNトラフィックを許可していません。
- C. サイト間VPNピアは異なる暗号化アルゴリズムを使用しています。
- D. サイト間VPN事前共有キーが一致していません。

正解: **A** ([コメントを发表する](#))

質問: 461

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

質問: 462

エンジニアは、LDAPがリスナーでクエリを受け入れることを有効にしました。悪意のある攻撃者がすべての有効な受信者をすばやく特定できないようにする必要があります。この目標を達成するには、Cisco ESAで何をする必要がありますか？

- A. バウンス検証を使用する
- B. 着信コンテンツフィルターを構成します。
- C. 受信者アクセステーブルのLDAPアクセスクエリをバイパスします。
- D. ディレクトリハーベスト攻撃防止を構成する

正解: B ([コメントを发表する](#))

説明

How do you create an LDAP group query on the ESA?

1. Create an LDAP group query under System Administration > LDAP.
2. Enable the group query for the listener under Network > Listener > {select the listener} > select the LDAP group query.
3. Go to Incoming Mail Policies.
4. Create a new policy for the group.
5. Add in the recipient matching the group.
6. Choose LDAP group query instead of email.
7. Select group query and put in the matching group name.
8. **Configure new incoming mail policies:** Anti-Spam, Anti-Virus, Content Filters, and Virus Outbreak Filters.

質問: 463

攻撃者は、相互に通信している2つのホストの間に、どのタイプの攻撃でマシンを挿入しますか？

- A. クロスサイトスクリプティング
- B. LDAPインジェクション
- C. 中間者
- D. 安全でないAPI

正解: ([正解を表示します](#))

質問: 464

ネットワーク管理者は、スイッチにダイナミックARPインスペクションを設定します。ダイナミックARPインスペクションが適用された後、そのスイッチのすべてのユーザーはどの宛先とも通信できなくなります。ネットワーク管理者は、すべてのインターフェイスのインターフェイスステータスを確認し、err-disabledインターフェイスはありません。この問題の原因は何ですか？

- A. DHCPスヌーピングがすべてのVLANで有効になっているわけではありません。
- B. ip arp Inspection limitコマンドがすべてのインターフェイスに適用され、すべてのユーザーのトラフィックをブロックしています。
- C. ダイナミックARPインスペクションがすべてのVLANで有効になっているわけではありません
- D. no ip arp Inspection trustコマンドがすべてのユーザーホストインターフェイスに適用されます

正解: ([正解を表示します](#))

質問: 465

Cisco ASA Netflow v9セキュアイベントロギングの特徴は何ですか？

- A. フロー作成、フローティアダウン、およびフロー拒否のイベントを追跡します。
- B. 特定のフローのすべてのレコードをエクスポートするステートレスIPフロー追跡を提供します。
- C. フローを継続的に追跡し、10秒ごとに更新を提供します。
- D. そのイベントはすべてのトラフィッククラスに並行して一致します。

正解: ([正解を表示します](#))

NetFlow Secure Event Logging (NSEL)のASAおよびASASM実装は、フロー内の重要なイベントを示すレコードのみをエクスポートするステートフルなIPフロートラッキング方式を提供します。追跡される重要なイベントには、flow-create、flow-teardown、およびflow-denied (Ethernet ACLによって拒否されたフローを除く)が含まれます。参照 <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html> 追跡される重要なイベントには次のものがあります。フロー作成、フローティアダウン、およびフロー拒否 (Ethernet ACLによって拒否されたフローを除く)。

```
Sysauthcontrol          Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                      = AUTHENTICATOR
PortControl              = FORCE_AUTHORIZED
ControlDirection        = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout            = 0
SuppTimeout              = 30
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
```

展示を参照してください。この出力を表示するために使用されたコマンドはどれですか？

- A. dot1xallを表示
- B. dot1xを表示
- C. dot1xのすべての概要を表示
- D. show dot1x interface gi1 / 0/12

正解: **A** ([コメントを发表する](#))

説明/リファレンス https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

質問: **468**

どのアルゴリズムが非対称暗号化を提供しますか？

- A. RC4
- B. AES
- C. 3DES
- D. RSA

正解: ([正解を表示します](#))

質問: **469**

組織は、クラウド環境でデータを保護したいと考えています。そのセキュリティモデルでは、すべてのユーザーが認証および承認される必要があります。アプリケーションとデータへのアクセスを許可または維持する前に、セキュリティの構成とポスチャを継続的に検証する必要があります。また、特定のアプリケーショントラフィックを許可し、デフォルトで他のすべてのトラフィックを拒否する必要があります。これらの要件を実装するには、どのテクノロジーを使用する必要がありますか？

- A. 仮想ルーティングと転送
- B. マイクロセグメンテーション
- C. アクセス制御ポリシー
- D. 仮想LAN

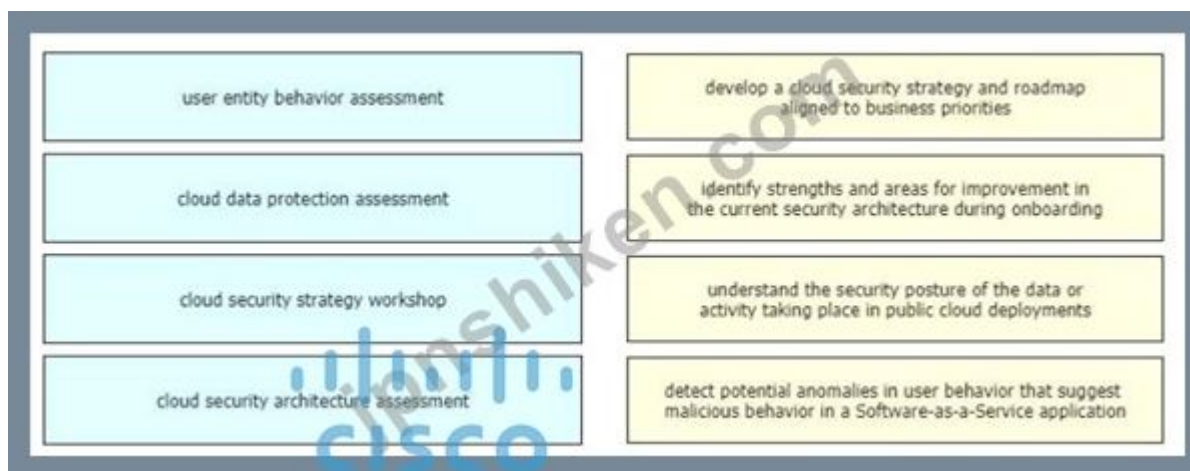
正解: ([正解を表示します](#))

ゼロトラストは、組織のネットワークの内外を問わず、すべてのユーザーが、アプリケーションやデータへのアクセスを許可または維持する前に、セキュリティ構成とポスチャについて認証、承認、および継続的に検証されることを要求するセキュリティフレームワークです。ゼロトラストは、従来のネットワークエッジがないことを前提としています。ネットワークは、ローカル、クラウド、または任意の場所のリソースとの組み合わせまたはハイブリッド、および任意の場所のワーカーにすることができます。

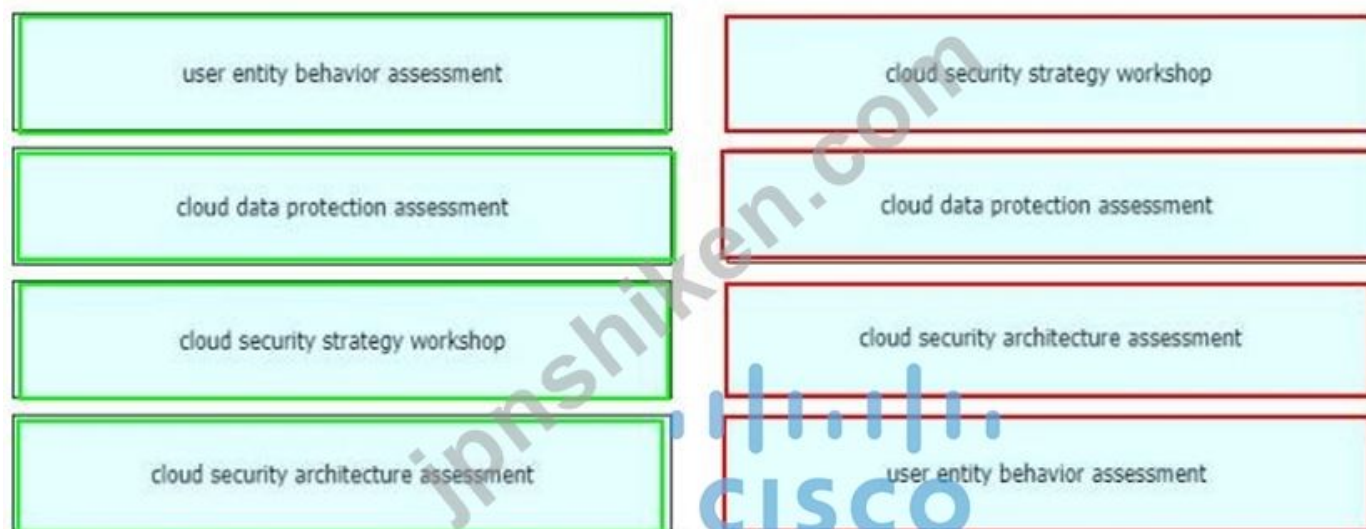
ゼロトラストモデルは、マイクロセグメンテーション ネットワークのすべての部分への個別のアクセスを維持するために境界を小さなゾーンに分割することを含むセキュリティ技術)を使用して、攻撃を封じ込めます。

質問: **470**

クラウドセキュリティ評価コンポーネントを左側から右側の定義にドラッグアンドドロップします。



正解:



質問: 471

同じベースEPGまたはuSegにある物理エンドポイントデバイスと仮想エンドポイントデバイスがVmwareVDSまたはMicrosoftvSwitchと相互に通信できないようにするオプションを提供する構成方法はどれですか。

- A. EPG間分離
- B. VLAN間セキュリティ
- C. 別々のEPGへの配置
- D. EPG内分離

正解: [\(正解を表示します\)](#)

質問: 472

Cisco Email Security Applianceの主な役割は何ですか？

- A. メールユーザーエージェント
- B. メール配信エージェント
- C. メール転送エージェント
- D. メール送信エージェント

正解: C ([コメントを发表する](#))

質問: 473

組織は、クラウド内のユーザー、データ、およびアプリケーションを保護したいと考えています。ソリューションはAPIベースであり、クラウドネイティブCASBとして動作する必要があります。この実装にはどのソリューションを使用する必要がありますか？

- A. Cisco Cloudlock
- B. Cisco Cloud Email Security
- C. CiscoFirepower次世代ファイアウォール
- D. Cisco Umbrella

正解: **A** ([コメントを發表する](#))

説明CiscoCloudlock :クラウドネイティブのクラウドアクセスセキュリティブローカー (CASB)とクラウドサイバーセキュリティプラットフォームを使用して、クラウドユーザー、データ、およびアプリケーションを保護します。参照 <https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf> Cisco Cloudlock :クラウドユーザーを保護します、データ、およびクラウドネイティブのクラウドアクセスセキュリティブローカー (CASB)とクラウドサイバーセキュリティプラットフォームを備えたアプリケーション。

参照 :

説明CiscoCloudlock :クラウドネイティブのクラウドアクセスセキュリティブローカー (CASB)とクラウドサイバーセキュリティプラットフォームを使用して、クラウドユーザー、データ、およびアプリケーションを保護します。参照 <https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf>

質問: **474**

AWSパブリッククラウド内にCiscoASAをデプロイするときにサポートされる機能はどれですか。

- A. IPv6
- B. レイヤー3ネットワークのユーザー展開
- C. マルチコンテキストモード
- D. クラスタリング

正解: ([正解を表示します](#))

質問: **475**

ネットワークエンジニアは、オンプレミスネットワーク内のユーザーとデバイスの動作を監視する必要があります。このデータは、分析のためにCiscoStealthwatchCloud分析プラットフォームに送信する必要があります。VMwareベースのハイパーバイザーにデプロイされたUbuntuベースのVMアプライアンスを使用して、この要件を満たすために何をする必要がありますか？

- A. syslogをCiscoStealthwatchCloudに送信するようにCiscoFMCを設定します
- B. CiscoStealthwatchCloudにデータを送信するCiscoStealthwatchCloudPNMセンサーを導入します
- C. Cisco FTDセンサーを導入して、ネットワークイベントをCiscoStealthwatchCloudに送信します
- D. NetFlowをCiscoStealthwatchCloudに送信するようにCiscoFMCを設定します

正解: ([正解を表示します](#))

Stealthwatch Cloudプライベートネットワークモニタリング (PNM) センサーは、非常に柔軟なテクノロジーであり、さまざまな展開シナリオで利用できます。さまざまなハイパーバイザー (VMware、VirtualBoxなど)に完全なUbuntuベースの仮想アプライアンスとしてデプロイできます。さまざまなLinuxベースのオペレーティングシステムを実行しているハードウェアに展開できます。

Stealthwatch Cloudプライベートネットワークモニタリング (PNM) センサーは、非常に柔軟なテクノロジーであり、さまざまな展開シナリオで利用できます。さまざまなハイパーバイザー (VMware、VirtualBoxなど)に完全なUbuntuベースの仮想アプライアンスとしてデプロイできます。さまざまなLinuxベースのオペレーティングシステムを実行しているハードウェアに展開できます。

参照 :

Stealthwatch Cloudプライベートネットワークモニタリング (PNM) センサーは、非常に柔軟なテクノロジーであり、さまざまな展開シナリオで利用できます。さまざまなハイパーバイザー (VMware、VirtualBoxなど) に完全なUbuntuベースの仮想アプライアンスとしてデプロイできます。さまざまなLinuxベースのオペレーティングシステムを実行しているハードウェアに展開できます。

質問: 476

XSS攻撃とSQLインジェクション攻撃の違いは何ですか？

- A. XSSはSQLデータベースを攻撃するために使用されるハッキング方法ですが、SQLインジェクション攻撃はさまざまな種類のアプリケーションに存在する可能性があります
- B. SQLインジェクション攻撃はデータベースから情報を盗むために使用されますが、XSS攻撃は、攻撃者がデータベースからデータを盗むことができるWebサイトにユーザーをリダイレクトするために使用されます
- C. SQLインジェクションはSQLデータベースを攻撃するために使用されるハッキング方法ですが、XSS攻撃はさまざまな種類のアプリケーションに存在する可能性があります
- D. XSS攻撃はデータベースから情報を盗むために使用されますが、SQLインジェクション攻撃は、攻撃者がデータを盗むことができるWebサイトにユーザーをリダイレクトするために使用されます

正解: ([正解を表示します](#))

質問: 477

Cisco Security Managerは何を管理していますか？

- A. Cisco ASA
- B. Cisco WSA
- C. Cisco WLC
- D. Cisco ESA

正解: ([正解を表示します](#))

<https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html>

質問: 478

ISE姿勢評価を使用してエンドポイントをチェックできる2つの条件はどれですか？ (2つ選択してください。)

- A. デフォルトのブラウザ
- B. ユーザーID
- C. Windowsファイアウォール
- D. コンピューターID
- E. Windowsサービス

正解: ([正解を表示します](#))

質問: 479

コンテキストディレクトリエージェントの機能は何ですか？

- A. ユーザーのグループメンバーシップを維持します
- B. WebセキュリティアプライアンスからActiveDirectoryにユーザー認証要求を中継します
- C. Active Directoryログを読み取り、IPアドレスをユーザー名にマップします
- D. ユーザー識別のためにWebセキュリティアプライアンスに代わってユーザー認証要求を受け入れます

正解: ([正解を表示します](#))

説明CiscoContextDirectory Agent (CDA)は、セキュリティゲートウェイがネットワーク内のどのユーザがどのIPアドレスを使用しているかを理解できるように、IPアドレスをユーザ名にマッピングするメカニズムです。これにより、これらのセキュリティゲートウェイは、これらのユーザ またはユーザが属するグループ)。CDAはCiscoLinuxマシンで実行されます。Active Directoryドメインコントローラー (DC)マシンのコレクションをリアルタイムで監視して、一般にユーザーのログインを示す認証関連のイベントを監視します。IPアドレスとユーザーIDのマッピングを学習、分析、およびデータベースにキャッシュします。最新のマッピングをコンシューマーデバイスで利用できるようにします。参照：

https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw

CDAはCiscoLinuxマシンで実行されます。Active Directoryドメインコントローラー (DC)マシンのコレクションをリアルタイムで監視して、一般にユーザーのログインを示す認証関連のイベントを監視します。IPアドレスとユーザーIDのマッピングを学習、分析、およびデータベースにキャッシュします。最新のマッピングをコンシューマーデバイスで利用できるようにします。

参照：

説明CiscoContextDirectory Agent (CDA)は、セキュリティゲートウェイがネットワーク内のどのユーザがどのIPアドレスを使用しているかを理解できるように、IPアドレスをユーザ名にマッピングするメカニズムです。これにより、これらのセキュリティゲートウェイは、これらのユーザ またはユーザが属するグループ)。CDAはCiscoLinuxマシンで実行されます。Active Directoryドメインコントローラー (DC)マシンのコレクションをリアルタイムで監視して、一般にユーザーのログインを示す認証関連のイベントを監視します。IPアドレスとユーザーIDのマッピングを学習、分析、およびデータベースにキャッシュします。最新のマッピングをコンシューマーデバイスで利用できるようにします。参照：

https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

質問: 480

エンジニアは、CiscoUmbrellを使用して特定のアドレスをブロックするようにポリシーを変更する必要があります。ポリシーはすでに作成されており、デフォルトのポリシー要素のu :としてアクティブになっています。このタスクを実行するには、他に何をする必要がありますか？

- A. アプリケーション設定を変更して、アプリケーションのみが必要なアドレスに接続できるようにします。
- B. コンテンツカテゴリを使用して、特定のアドレスをブロックまたは許可します。
- C. 指定したアドレスをIDリストに追加し、ブロックアクションを作成します。
- D. 許可またはブロックするアドレスの宛先リストを作成します。

正解: A ([コメントを發表する](#))

質問: 481

共有アプライアンスで管理を分離できるASA展開モードはどれですか。

- A. マルチコンテキストモード
- B. DMZマルチゾーンモード
- C. 透過ファイアウォールモード
- D. ルーテッドモード

正解: ([正解を表示します](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **482**

フィッシング攻撃からユーザーを保護するエンドポイントソリューションはどれですか？

- A. Cisco Identity Services Engine
- B. シス CiscoAnyConnectとNetworkAccessManagerモジュール
- C. UmbrellaRoamingSecurityモジュールを備えたCiscoAnyConnect
- D. ISEポスチャモジュールを備えたCisco AnyConnect

正解: ([正解を表示します](#))

質問: **483**

シスコおよびその他の業界組織が既知のセキュリティの発見と脆弱性を公開してユーザーに通知する場合、どの名前が使用されますか？

- A. 一般的な脆弱性とエクスポージャー
- B. 一般的なエクスプロイトと脆弱性
- C. 一般的なセキュリティエクスプロイト
- D. 一般的な脆弱性、エクスプロイト、脅威

正解: ([正解を表示します](#))

<https://www.cisco.com/c/en>

質問: **484**

AES暗号化の2つの説明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. AESは3DESよりも安全性が低くなります。
- B. AESは暗号化に256ビットキーを使用できます。
- C. AESは3DESよりも安全です。
- D. AESは暗号化に168ビットキーを使用できます。
- E. AESは、キーを3回順番に暗号化および復号化します。

正解: ([正解を表示します](#))

質問: **485**

Firepower Next Generation Intrusion Prevention System検出器を、左側から右側の正しい定義にドラッグアンドドロップします。

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

正解:

PortScan Detection	Distributed PortScan
Port Sweep	Decoy PortScan
Decoy PortScan	Port Sweep
Distributed PortScan	PortScan Detection

質問: 486

クロスサイトスクリプティングを制御するために使用される2つの予防策はどれですか？ 2つ選択してください。）

- A. ドメインごとにクライアント側のスクリプトを有効にします。
- B. コンテキスト出力のエンコーディング/エスケープを組み込みます。
- C. HTML検査エンジンでCookie検査を無効にします。
- D. 信頼できないHTML入力をHTMLサニタイズエンジンを介して実行します。
- E. SameSitecookie属性は使用しないでください。

正解: [\(正解を表示します\)](#)

説明/参照 :

質問: 487

Firepower Next Generation Intrusion Prevention System検出器を、左側から右側の正しい定義にドラッグアンドドロップします。

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

正解:



質問: 488

CiscoASA5500シリーズファイアウォールでNetFlowを許可する2つのタスクはどれですか。(2つ選択してください。)

- A. flow-exportコマンドを使用してNetFlowコレクターを定義します。
- B. NetFlowバージョン9を有効にします。
- C. 興味深いトラフィックに一致するクラスマップを作成します。
- D. NetFlowExporterをインバウンド方向の外部インターフェイスに適用します。
- E. ポート9996でUDPトラフィックを許可するACLを作成します。

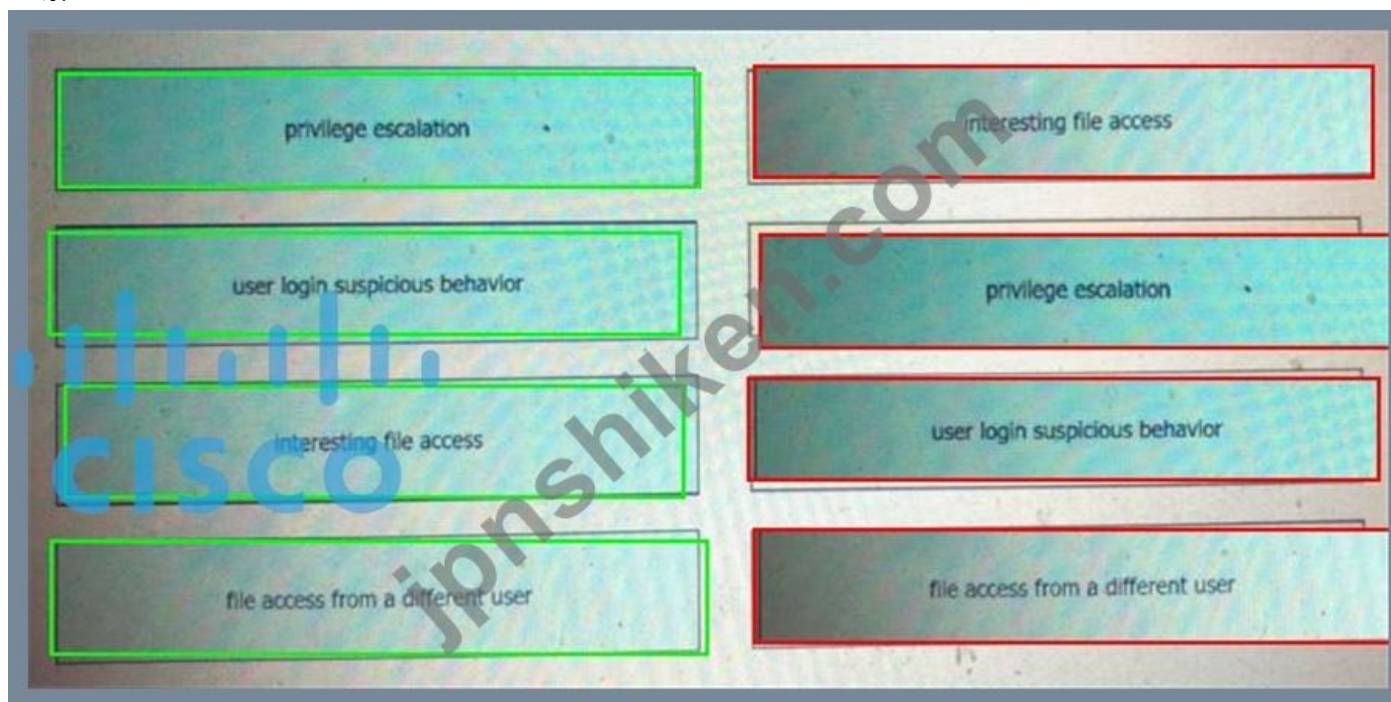
正解: [\(正解を表示します\)](#)

質問: 489

Cisco Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグアンドドロップします。



正解:



質問: 490

CおよびC++プログラミング言語に一般的に関連する攻撃はどれですか？

- A. クロスサイトスクリプティング
- B. ウォーターホール
- C. DDoS
- D. バッファオーバーフロー

正解: (正解を表示します)

バッファオーバーフロー (またはバッファオーバーラン)は、データの量がメモリバッファのストレージ容量を超えると発生します。その結果、バッファにデータを書き込もうとするプログラムは、隣接するメモリ位置を上書きします。

バッファオーバーフローは、CおよびC++の低レベルコードの脆弱性です。攻撃者は、プログラムをクラッシュさせたり、データを破損させたり、個人情報盗んだり、自分のコードを実行したりする可能性があります。これは基本的に、割り当てられたメモリスペース外のバッファにアクセスすることを意味します。これは、アレイの場合に非常に頻繁に発生します。

質問: 491

最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

- A. アクセスポリシーを変更します。
- B. 識別プロファイルを変更します。
- C. アウトバウンドマルウェアスキャンポリシーを変更する
- D. Webプロキシ設定を変更する

正解: ([正解を表示します](#))

説明

An explicit proxy deployment is when a client proxy-aware application, like a mature web browser, has a configuration area within for proxy settings to declare and use a proxy, like the WSA. This method is typically combined with a firewall restricting web traffic that does not originate from the WSA's IP to prevent users from circumventing web policy controls and accessing

質問: 492

CiscoASAプラットフォームで有効なRESTAPIの2つの要求はどれですか。(2つ選択してください。)

- A. オプション
- B. 置く
- C. 接続
- D. プッシュ
- E. 取得

正解: B,E ([コメントを發表する](#))

質問: 493

セキュリティイベントのみをログに記録するようにCiscoUmbrellaを構成するにはどうすればよいですか。

- A. [セキュリティ設定]セクション
- B. [展開]セクションのネットワークごと
- C. レポート設定で
- D. ポリシーごと

正解: ([正解を表示します](#))

質問: 494

交通嵐制御行動の特徴は何ですか？

- A. トラフィックストーム制御は、パケット送信元アドレスの個別/グループビットを使用して、パケットがユニキャストかブロードキャストかを判別します。
- B. トラフィックストーム制御は、10秒間のトラフィックストーム制御間隔で着信トラフィックレベルを監視します。

C. トラフィックストーム制御は、結合されたトラフィックが間隔内のレベルを超えた場合、すべてのブロードキャストおよびマルチキャストトラフィックをドロップします。

D. トラフィックストーム制御は、パケットがユニキャストであるかブロードキャストであるかを判別できません。

正解: ([正解を表示します](#))

質問: **495**

コンテキストディレクトリエージェントの機能は何ですか？

A. ユーザーのグループメンバーシップを維持します

B. WebセキュリティアプライアンスからActiveDirectoryにユーザー認証要求を中継します

C. Active Directoryログを読み取り、IPアドレスをユーザー名にマップします

D. ユーザー識別のためにWebセキュリティアプライアンスに代わってユーザー認証要求を受け入れます

正解: **C** ([コメントを発表する](#))

Cisco Context Directory Agent (CDA)は、セキュリティゲートウェイがネットワーク内のどのユーザがどのIPアドレスを使用しているかを理解できるように、IPアドレスをユーザ名にマッピングするメカニズムです。これにより、これらのセキュリティゲートウェイは、これらのユーザ またはユーザが属するグループ)。

CDAはCiscoLinuxマシンで実行されます。Active Directoryドメインコントローラー (DC)マシンのコレクションをリアルタイムで監視して、一般にユーザーのログインを示す認証関連のイベントを監視します。IPアドレスとユーザーIDのマッピングを学習、分析、およびデータベースにキャッシュします。最新のマッピングをコンシューマーデバイスで利用できるようにします。

Cisco Context Directory Agent (CDA)は、セキュリティゲートウェイがネットワーク内のどのユーザがどのIPアドレスを使用しているかを理解できるように、IPアドレスをユーザ名にマッピングするメカニズムです。これにより、これらのセキュリティゲートウェイは、これらのユーザ またはユーザが属するグループ)。

CDAはCiscoLinuxマシンで実行されます。Active Directoryドメインコントローラー (DC)マシンのコレクションをリアルタイムで監視して、一般にユーザーのログインを示す認証関連のイベントを監視します。IPアドレスとユーザーIDのマッピングを学習、分析、およびデータベースにキャッシュします。最新のマッピングをコンシューマーデバイスで利用できるようにします。

参照：

[cda_oveviw.html](#)

Cisco Context Directory Agent (CDA)は、セキュリティゲートウェイがネットワーク内のどのユーザがどのIPアドレスを使用しているかを理解できるように、IPアドレスをユーザ名にマッピングするメカニズムです。これにより、これらのセキュリティゲートウェイは、これらのユーザ またはユーザが属するグループ)。

CDAはCiscoLinuxマシンで実行されます。Active Directoryドメインコントローラー (DC)マシンのコレクションをリアルタイムで監視して、一般にユーザーのログインを示す認証関連のイベントを監視します。IPアドレスとユーザーIDのマッピングを学習、分析、およびデータベースにキャッシュします。最新のマッピングをコンシューマーデバイスで利用できるようにします。

[cda_oveviw.html](#)

質問: **496**

エンジニアがIPsecVPNを構成しており、信頼性が高く、ACKとシーケンスをサポートする認証プロトコルが必要です。どのプロトコルがこの目標を達成しますか？

A. AES-192

B. AES-256

C. IKEv1

D. ESP

正解: **D** ([コメントを发表する](#))

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 497

Cisco Advanced Phishing Protectionはどのようにユーザーを保護しますか？

- A. 機械学習とリアルタイムの行動分析を使用します。
- B. メッセージを安全に送信するセンサーを利用しています。
- C. DKIMを使用して送信者を検証します。
- D. 送信者がどのIDを認識するかを決定します

正解: ([正解を表示します](#))

質問: 498

Cisco ESA管理者は、隔離された電子メールが配信される前にウイルスがないことを確認するようにCiscoESAを設定する必要があります。さらに、既知の不良メールサーバーからのメールの配信を防止する必要があります。これらの要件を満たすために実行する必要がある2つのアクションはどれですか？ 2つ選択してください)

- A. SenderBaseのアウトブレイクフィルターを使用する
- B. メッセージ追跡サービスを有効にする
- C. 受信者アクセステーブルを設定します
- D. CiscoESAをDMZに導入します
- E. アンチウイルス署名を使用して隔離された電子メールをスキャンする

正解: ([正解を表示します](#))

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注 :ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせ

ずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

参照：

b_ESA_Admin_Guide_12_0 / b_ESA_Admin_Guide_12_0_chapter_0100100.html

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

注：リモートアクセストロイの木馬（RAT）と混同しないように、受信者アクセステーブル（RAT）は、パブリックリスナーが受け入れる受信者を定義するCisco ESA用語です。

ウイルス対策署名を使用して電子メールをスキャンし、電子メールにウイルスが添付されていないことを確認する必要があります。

注：ウイルス署名は、ウイルスのフィンガープリントです。これは、識別を可能にする一意のデータのセット、またはコードのビットです。ウイルス対策ソフトウェアは、ウイルス署名を使用してコンピュータファイルシステム内のウイルスを検出し、ウイルスの検出、隔離、および削除を可能にします。SenderBaseは、電子メール管理者が送信者を調査し、正当な電子メールの送信元を特定し、スパマーをブロックするのに役立つように設計された電子メールレピュテーションサービスです。Cisco ESAは、既知の送信者または信頼性の高い送信者からメッセージを受信すると、コンテンツをスキャンせずにエンドユーザーに直接メッセージを配信します。ただし、Cisco ESAは、不明または信頼性の低い送信者から電子メールメッセージを受信すると、スパム対策およびウイルス対策スキャンを実行します。

b_ESA_Admin_Guide_12_0 / b_ESA_Admin_Guide_12_0_chapter_0100100.html

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

b_ESA_Admin_Guide_12_0 / b_ESA_Admin_Guide_12_0_chapter_0100100.html

->したがって、アウトブレイクフィルタを使用して、不良メールサーバーからの電子メールをブロックできます。

Webサーバーと電子メールゲートウェイは通常DMZに配置されているため、

注：リモートアクセストロイの木馬（RAT）と混同しないように、受信者アクセステーブル（RAT）は、パブリックリスナーが受け入れる受信者を定義するCisco ESA用語です。

質問: 499

Cisco SDNアーキテクチャ内のノースバウンドAPIとサウスバウンドAPIの2つの機能は何ですか。（2つ選択してください。）

- A. サウスバウンドインターフェイスは、VLANやIPアドレスなどのデバイス構成を利用します。
- B. ノースバウンドインターフェイスは、OpenFlowとOpFlexを利用してネットワークデバイスと統合します。
- C. サウスバウンドAPIは、CLI、SNMP、およびRESTCONFを利用します。
- D. サウスバウンドAPIは、SDNコントローラーをアプリケーションと統合する方法を定義するために使用されます。
- E. ノースバウンドAPIは、GET、POST、DELETEなどのRESTful APIメソッドを利用します。

正解: ([正解を表示します](#))

質問: 500

AWSパブリッククラウド内にCisco ASAvをデプロイするときにサポートされる機能はどれですか。

- A. マルチコンテキストモード
- B. レイヤー3ネットワークのユーザー展開
- C. IPv6
- D. クラスタリング

正解: ([正解を表示します](#))

説明AWS上のASAvは、次の機能をサポートしています。+次世代のAmazon EC2ComputeOptimizedインスタンスファミリーであるAmazonEC2C5インスタンスのサポート。+仮想プライベートクラウド (VPC)での展開+利用可能な場合は拡張ネットワーキング (SR-IOV)+Amazonマーケットプレイスからの展開+インスタンスあたり最大4つのvCPU+ L3ネットワークのユーザー展開+ルーテッドモード (デフォルト) 注Cisco Adaptive Security仮想アプライアンス (ASAv)は、物理Cisco ASAと同じソフトウェアを実行して、実証済みのセキュリティ機能を仮想フォームファクタで提供します。ASAvはパブリックAWSクラウドにデプロイできます。次に、時間の経過とともに場所を拡大、縮小、またはシフトする仮想および物理データセンターのワークロードを保護するように構成できます。参照 <https://www.cisco.com>。

+次世代のAmazonEC2ComputeOptimizedインスタンスファミリーであるAmazonEC2C5インスタンスのサポート。

+仮想プライベートクラウド (VPC)での展開

+利用可能な場合は拡張ネットワーキング (SR-IOV)

+Amazonマーケットプレイスからのデプロイ

+インスタンスあたり最大4つのvCPU

+L3ネットワークのユーザー展開

+ルーテッドモード (デフォルト)

注 Cisco Adaptive Security仮想アプライアンス (ASAv)は、物理Cisco ASAと同じソフトウェアを実行して、実証済みのセキュリティ機能を仮想フォームファクタで提供します。ASAvはパブリックAWSクラウドにデプロイできます。

説明AWS上のASAvは、次の機能をサポートしています。+次世代のAmazon EC2ComputeOptimizedインスタンスファミリーであるAmazonEC2C5インスタンスのサポート。+仮想プライベートクラウド (VPC)での展開+利用可能な場合は拡張ネットワーキング (SR-IOV)+Amazonマーケットプレイスからの展開+インスタンスあたり最大4つのvCPU+ L3ネットワークのユーザー展開+ルーテッドモード (デフォルト) 注Cisco Adaptive Security仮想アプライアンス (ASAv)は、物理Cisco ASAと同じソフトウェアを実行して、実証済みのセキュリティ機能を仮想フォームファクタで提供します。ASAvはパブリックAWSクラウドにデプロイできます。次に、時間の経過とともに場所を拡大、縮小、またはシフトする仮想および物理データセンターのワークロードを保護するように構成できます。参照 <https://www.cisco.com>。

質問: 501

マネージドIntercloudFabricデプロイメントモデルの2つのタイプは何ですか？ (2つ選択してください)

A. サービスプロバイダーが管理

B. パブリックマネージド

C. ハイブリッドマネージド

D. ユーザー管理

E. エンタープライズ管理

正解: ([正解を表示します](#))

多くの企業は、主に利便性と迅速な展開のために、開発ワークロードをパブリッククラウドに展開することを好みます。このアプローチは、ITトラフィックと支出の流れを制御し、データと知的財産のセキュリティを確保するのに役立つIT管理者に懸念を引き起こす可能性があります。適切な管理がなければ、データと知的財産はこの見落としから逃れることができます。Cisco Intercloud Fabricソリューションは、このシャドーITを制御し、IT制御の外部でパブリッククラウドに展開されているリソースを検出し、これらのリソースをCiscoIntercloudFabricの制御下に置くのに役立ちます。Cisco Intercloud Fabricは、2つのハイブリッドクラウド導入モデルに適したクラウド導入要件に対応しています。エンタープライズマネージド (エンタープライズは独自のクラウド環境を管理します)およびサービスプロバイダーマネージド (サービスプロバイダーはすべてのクラウドリソースを管理および制御します)。参照 https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric.pdf Cisco Intercloud Fabricアーキテクチャは、次の2つの消費モデルに対応する2つの製品構成を提供します。Intercloud Fabric for Business + Cisco Intercloud Fabric for Providersリファレンス https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_2.html

質問: 502

機能を左側から右側の正しいテクノロジーにドラッグアンドドロップします。

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

正解:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

説明

superior threat prevention and mitigation for known and unknown threats
detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions

質問: 503

アプリケーションの可視性とセグメンテーションにより、ハイブリッドクラウド展開のワークロードを保護するソリューションはどれですか？

- A. 火力
- B. ステルスウォッチ
- C. ネクサス
- D. テトレーション

正解: D (コメントを发表する)

質問: 504

Easy ConnectをCiscoTrustSecと併用した場合、ネットワークアクセスの制御に役立つ2つの方法はどれですか。 2つ選択してください)

- A. 複数のセキュリティ製品が情報を共有し、連携してネットワークのセキュリティ体制を強化できるようにします。
- B. 接続されているすべてのエンドポイントの完全な可視性を提供するダッシュボードをCiscoISEに作成します。
- C. セキュリティグループタグの割り当てが可能であり、スイッチまたはエンドポイントで802.1xを設定する必要はありません。
- D. サードパーティ製品と統合して、ネットワーク全体の可視性を向上させます。
- E. ADに対して認証される管理対象エンドポイントをセキュリティグループ (PassiveID)にマッピングできます。

正解: C,E ([コメントを发表する](#))

Easy Connectは、有線接続または無線接続のどちらを使用する場合でも、エンドポイントで802.1Xを必要とせずに、セキュリティグループタグをエンドポイントに割り当てることができるため、ネットワークアクセスの制御とセグメンテーションを簡素化します。

Easy Connectは、有線接続または無線接続のどちらを使用する場合でも、エンドポイントで802.1Xを必要とせずに、セキュリティグループタグをエンドポイントに割り当てることができるため、ネットワークアクセスの制御とセグメンテーションを簡素化します。

参照 :

Easy Connectは、有線接続または無線接続のどちらを使用する場合でも、エンドポイントで802.1Xを必要とせずに、セキュリティグループタグをエンドポイントに割り当てることができるため、ネットワークアクセスの制御とセグメンテーションを簡素化します。

質問: 505

Firepower Next Generation Intrusion Prevention Systemで使用されている2つのアプリケーション層プリプロセッサはどれですか？ 2つ選択してください)

- A. パケットデコーダー
- B. SIP
- C. modbus
- D. インライン正規化
- E. SSL

正解: ([正解を表示します](#))

アプリケーション層プロトコルは、さまざまな方法で同じデータを表すことができます。Firepowerシステムは、特定のタイプのパケットデータを侵入ルールエンジンが分析できる形式に正規化するアプリケーション層プロトコルデコーダーを提供します。アプリケーション層のプロトコルエンコーディングを正規化することで、ルールエンジンは、データの表現方法が異なるパケットに同じコンテンツ関連のルールを効果的に適用し、意味のある結果を得ることができます。

アプリケーション層プロトコルは、さまざまな方法で同じデータを表すことができます。Firepowerシステムは、特定のタイプのパケットデータを侵入ルールエンジンが分析できる形式に正規化するアプリケーション層プロトコルデコーダーを提供します。アプリケーション層のプロトコルエンコーディングを正規化することで、ルールエンジンは、データの表現方法が異なるパケットに同じコンテンツ関連のルールを効果的に適用し、意味のある結果を得ることができます。

参照 :

FirePowerは、DNS、FTP / Telnet、SIP、SSL、SMTP、SSHプリプロセッサを含む多くのプリプロセッサを使用します。

アプリケーション層プロトコルは、さまざまな方法で同じデータを表すことができます。Firepowerシステムは、特定のタイプのパケットデータを侵入ルールエンジンが分析できる形式に正規化するアプリケーション層プロトコルデコーダーを提供します。アプリケーション層のプロトコルエンコーディングを正規化することで、ルールエンジンは、データの表現方法が異なるパケットに同じコンテンツ関連のルールを効果的に適用し、意味のある結果を得ることができます。

FirePowerは、DNS、FTP / Telnet、SIP、SSL、SMTP、SSHプリプロセッサを含む多くのプリプロセッサを使用します。

質問: **506**

セキュリティイベントのみをログに記録するようにCiscoUmbrellaを構成するにはどうすればよいですか。

- A. ポリシーごと
- B. レポート設定で
- C. [セキュリティ設定]セクション
- D. [展開]セクションのネットワークごと

正解: ([正解を表示します](#))

IDのアクティビティのログは、最初にポリシーを作成するときにポリシーごとに設定されます。デフォルトでは、ロギングがオンになっており、IDが宛先に到達するために行うすべてのリクエストをログに記録するように設定されています。ポリシーを作成した後はいつでも、Umbrellaがログに記録するIDアクティビティのレベルを変更できます。ポリシーウィザードからのログ設定は次のとおりです。すべてのリクエストをログに記録するコンテンツ、セキュリティ、その他のいずれの場合でも、完全なログ記録の場合ログのみのセキュリティイベントセキュリティログのみの場合、ユーザーのプライバシーが向上しますローミングクライアントを使用するユーザーに適した設定個人のデバイスにインストールされているリクエストをログに記録しないすべてのログを無効にします。このオプションを選択した場合、レポートするログが何もないため、このポリシーを使用したIDのほとんどのレポートは役に立ちません。参照 <https://docs.umbrella.com/deployment-umbrella/docs/log-management>ポリシーウィザードから、すべてのリクエストをログに記録するコンテンツ、セキュリティ、またはその他の方法で完全にログに記録するセキュリティイベントのみをログに記録するセキュリティログのみに使用するため、ユーザーのプライバシーが向上しますローミングクライアントが個人のデバイスにインストールされているユーザーに適した設定ログに記録しないでくださいリクエストすべてのログを無効にします。このオプションを選択した場合、レポートするログが何もないため、このポリシーを使用したIDのほとんどのレポートは役に立ちません。

IDのアクティビティのログは、最初にポリシーを作成するときにポリシーごとに設定されます。デフォルトでは、ロギングがオンになっており、IDが宛先に到達するために行うすべてのリクエストをログに記録するように設定されています。ポリシーを作成した後はいつでも、Umbrellaがログに記録するIDアクティビティのレベルを変更できます。ポリシーウィザードからのログ設定は次のとおりです。すべてのリクエストをログに記録するコンテンツ、セキュリティ、その他のいずれの場合でも、完全なログ記録の場合ログのみのセキュリティイベントセキュリティログのみの場合、ユーザーのプライバシーが向上しますローミングクライアントを使用するユーザーに適した設定個人のデバイスにインストールされているリクエストをログに記録しないすべてのログを無効にします。このオプションを選択した場合、レポートするログが何もないため、このポリシーを使用したIDのほとんどのレポートは役に立ちません。参照 <https://docs.umbrella.com/deployment-umbrella/docs/log-management>

質問: **507**

シスコおよびその他の業界組織が既知のセキュリティの発見と脆弱性を公開してユーザーに通知する場合、どの名前が使用されますか？

- A. 一般的な脆弱性とエクスポージャー
- B. 一般的なエクспロイトと脆弱性
- C. 一般的なセキュリティエクспロイト
- D. 一般的な脆弱性、エクспロイト、脅威

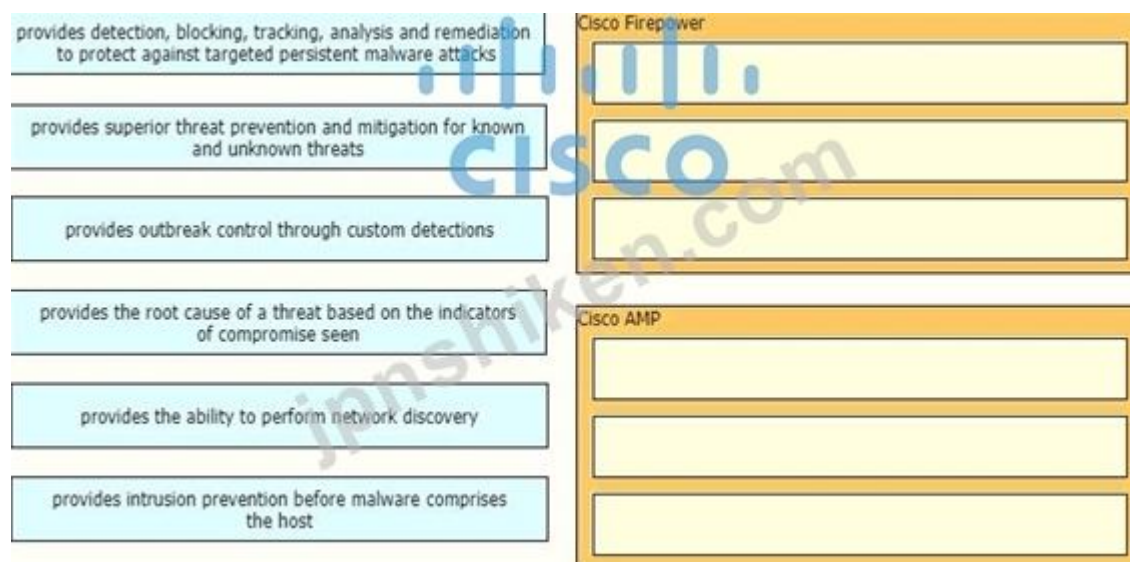
正解: ([正解を表示します](#))

参照 :

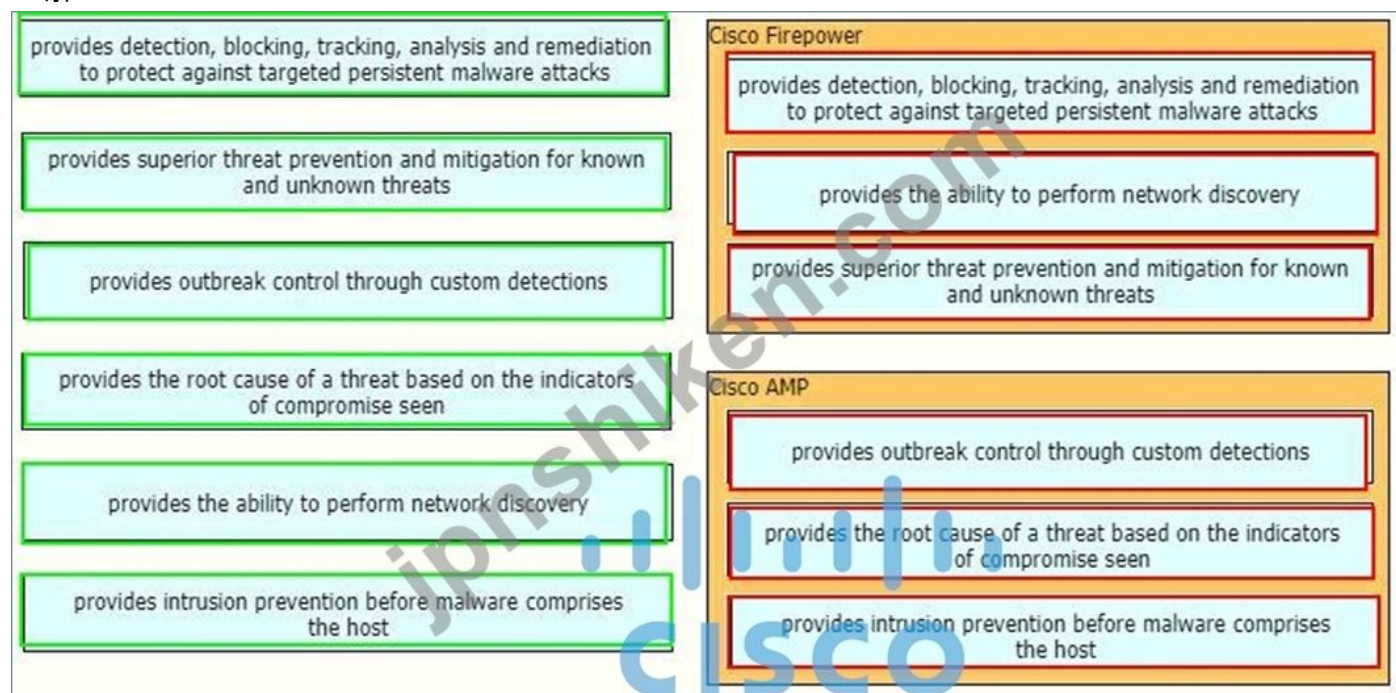
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cve/174/cve-addressed-1741.html>

質問: **508**

CiscoFirepowerとCiscoAMPの機能を左側から右側の適切なカテゴリにドラッグアンドドロップします。



正解:



質問: 509

CiscoDNACenterを使用して実行できる2つのアクティビティはどれですか。2つ選択してください)

- A. DHCP
- B. デザイン
- C. 会計
- D. DNS
- E. プロビジョニング

正解: B,E ([コメントを发表する](#))

Cisco DNA Centerには、ITワークフローに合わせた4つの一般的なセクションがあります。

設計 :デバイスおよびサイトごとに一貫した構成になるようにネットワークを設計します。物理マップと論理トポロジは、視覚的な参照をすばやく提供するのに役立ちます。直接インポート機能は、既存のマップ、イメージ、およびトポロジをCiscoPrimeInfrastructureおよびCiscoApplicationPolicy Infrastructure Controller Enterprise Module (APIC-EM)から直接取り込み、アップグレードを簡単かつ迅速に行えるようにします。サイトごとのデバイ

ス構成は、新しいネットワークデバイスを自動的にプロビジョニングするために使用できる「ゴールデンイメージ」に統合できます。これらの新しいデバイスは、デバイスの詳細を関連付けてサイトにマッピングすることにより、事前にステージングすることができます。または、接続時に要求してサイトにマッピングすることもできます。

ポリシー :ビジネスインテントをネットワークポリシーに変換し、アクセス制御、トラフィックルーティング、サービス品質などのポリシーを有線および無線インフラストラクチャ全体に一貫して適用します。ポリシーベースのアクセス制御とネットワークセグメンテーションは、CiscoDNACenterとCiscoIdentityServices Engine (ISE)から構築されたCisco Software-Defined Access (SDAccess)ソリューションの重要な機能です。CiscoDNACenterで実行されているCiscoAINetworkAnalyticsおよびCiscoGroup-BasedPolicy Analyticsは、エンドポイントを識別し、類似のエンドポイントをグループ化し、グループの通信動作を決定します。次に、Cisco DNA Centerは、各グループのメンバー間およびメンバー内で許可される通信の形式を決定するポリシーの作成を容易にします。次に、ISEは基盤となるインフラストラクチャをアクティブ化し、ネットワークをセグメント化して仮想オーバーレイを作成し、これらのポリシーに一貫して従います。このようなセグメント化は、職場でゼロトラストセキュリティを実装し、リスクを軽減し、脅威を封じ込め、エンドポイントに必要な適切なレベルのアクセスを提供することで、規制コンプライアンスの検証に役立ちます。

プロビジョニング :Cisco DNA Centerでポリシーを作成したら、プロビジョニングは単純なドラッグアンドドロップタスクです。

Cisco DNA Centerインベントリリストのプロファイル（スケーラブルグループタグまたは「SGT」と呼ばれる）にはポリシーが割り当てられ、このポリシーは常にIDに従います。プロセスは完全に自動化されており、ゼロタッチです。ネットワークに追加された新しいデバイスは、IDに基づいてSGTに割り当てられます。これにより、リモートオフィスのセットアップが大幅に容易になります。

アシュアランス :Cisco DNA Assuranceは、AI / MLを使用して、ネットワーク上のすべてのポイントをセンサーにし、アプリケーションのパフォーマンスとユーザー接続に関する継続的なストリーミングテレメトリをリアルタイムで送信します。クリーンでシンプルなダッシュボードには、詳細なネットワークヘルスとフラグの問題が表示されます。次に、ガイド付き修復により解決が自動化され、日常的なトラブルシューティング作業が少なくなり、ネットワークのパフォーマンスが最適に保たれます。

その結果、一貫したエクスペリエンスとネットワークのプロアクティブな最適化が実現し、タスクのトラブルシューティングに費やす時間が短縮されます。

Cisco DNA Centerには、ITワークフローに合わせた4つの一般的なセクションがあります。

設計 :デバイスおよびサイトごとに一貫した構成になるようにネットワークを設計します。物理マップと論理トポロジは、視覚的な参照をすばやく提供するのに役立ちます。直接インポート機能は、既存のマップ、イメージ、およびトポロジをCiscoPrimeInfrastructureおよびCiscoApplicationPolicy Infrastructure Controller Enterprise Module (APIC-EM)から直接取り込み、アップグレードを簡単かつ迅速に行えるようにします。サイトごとのデバイス構成は、新しいネットワークデバイスを自動的にプロビジョニングするために使用できる「ゴールデンイメージ」に統合できます。これらの新しいデバイスは、デバイスの詳細を関連付けてサイトにマッピングすることにより、事前にステージングすることができます。または、接続時に要求してサイトにマッピングすることもできます。

ポリシー :ビジネスインテントをネットワークポリシーに変換し、アクセス制御、トラフィックルーティング、サービス品質などのポリシーを有線および無線インフラストラクチャ全体に一貫して適用します。ポリシーベースのアクセス制御とネットワークセグメンテーションは、CiscoDNACenterとCiscoIdentityServices Engine (ISE)から構築されたCisco Software-Defined Access (SDAccess)ソリューションの重要な機能です。CiscoDNACenterで実行されているCiscoAINetworkAnalyticsおよびCiscoGroup-BasedPolicy Analyticsは、エンドポイントを識別し、類似のエンドポイントをグループ化し、グループの通信動作を決定します。次に、Cisco DNA Centerは、各グループのメンバー間およびメンバー内で許可される通信の形式を決定するポリシーの作成を容易にします。次に、ISEは基盤となるインフラストラクチャをアクティブ化し、ネットワークをセグメント化して仮想オーバーレイを作成し、これらのポリシーに一貫して従います。このようなセグメント化は、職場でゼロトラストセキュリティを実装し、リスクを軽減し、脅威を封じ込め、エンドポイントに必要な適切なレベルのアクセスを提供することで、規制コンプライアンスの検証に役立ちます。

プロビジョニング :Cisco DNA Centerでポリシーを作成したら、プロビジョニングは単純なドラッグアンドドロップタスクです。

Cisco DNA Centerインベントリリストのプロファイル スケーラブルグループタグまたは SGT」と呼ばれる)にはポリシーが割り当てられ、このポリシーは常にIDに従います。プロセスは完全に自動化されており、ゼロタッチです。ネットワークに追加された新しいデバイスは、IDに基づいてSGTに割り当てられます。これにより、リモートオフィスのセットアップが大幅に容易になります。

アシュアランス :Cisco DNA Assuranceは、AI / MLを使用して、ネットワーク上のすべてのポイントをセンサーにし、アプリケーションのパフォーマンスとユーザー接続に関する継続的なストリーミングテレメトリをリアルタイムで送信します。クリーンでシンプルなダッシュボードには、詳細なネットワークヘルスとフラグの問題が表示されます。次に、ガイド付き修復により解決が自動化され、日常的なトラブルシューティング作業が少なくなり、ネットワークのパフォーマンスが最適に保たれます。

その結果、一貫したエクスペリエンスとネットワークのプロアクティブな最適化が実現し、タスクのトラブルシューティングに費やす時間が短縮されます。

参照：

Cisco DNA Centerには、ITワークフローに合わせた4つの一般的なセクションがあります。

設計 :デバイスおよびサイトごとに一貫した構成になるようにネットワークを設計します。物理マップと論理トポロジは、視覚的な参照をすばやく提供するのに役立ちます。直接インポート機能は、既存のマップ、イメージ、およびトポロジをCiscoPrimeInfrastructureおよびCiscoApplicationPolicy Infrastructure Controller Enterprise Module (APIC-EM)から直接取り込み、アップグレードを簡単かつ迅速に行えるようにします。サイトごとのデバイス構成は、新しいネットワークデバイスを自動的にプロビジョニングするために使用できる 「ボールデンイメージ」に統合できます。これらの新しいデバイスは、デバイスの詳細を関連付けてサイトにマッピングすることにより、事前にステージングすることができます。または、接続時に要求してサイトにマッピングすることもできます。

ポリシー :ビジネスインテントをネットワークポリシーに変換し、アクセス制御、トラフィックルーティング、サービス品質などのポリシーを有線および無線インフラストラクチャ全体に一貫して適用します。ポリシーベースのアクセス制御とネットワークセグメンテーションは、CiscoDNACenterとCiscoIdentityServices Engine (ISE)から構築されたCisco Software-Defined Access (SDAccess)ソリューションの重要な機能です。CiscoDNACenterで実行されているCiscoAINetworkAnalyticsおよびCiscoGroup-BasedPolicy Analyticsは、エンドポイントを識別し、類似のエンドポイントをグループ化し、グループの通信動作を決定します。次に、Cisco DNA Centerは、各グループのメンバー間およびメンバー内で許可される通信の形式を決定するポリシーの作成を容易にします。次に、ISEは基盤となるインフラストラクチャをアクティブ化し、ネットワークをセグメント化して仮想オーバーレイを作成し、これらのポリシーに一貫して従います。このようなセグメント化は、職場でゼロトラストセキュリティを実装し、リスクを軽減し、脅威を封じ込め、エンドポイントに必要な適切なレベルのアクセスを提供することで、規制コンプライアンスの検証に役立ちます。

プロビジョニング :Cisco DNA Centerでポリシーを作成したら、プロビジョニングは単純なドラッグアンドドロップタスクです。

Cisco DNA Centerインベントリリストのプロファイル スケーラブルグループタグまたは SGT」と呼ばれる)にはポリシーが割り当てられ、このポリシーは常にIDに従います。プロセスは完全に自動化されており、ゼロタッチです。ネットワークに追加された新しいデバイスは、IDに基づいてSGTに割り当てられます。これにより、リモートオフィスのセットアップが大幅に容易になります。

アシュアランス :Cisco DNA Assuranceは、AI / MLを使用して、ネットワーク上のすべてのポイントをセンサーにし、アプリケーションのパフォーマンスとユーザー接続に関する継続的なストリーミングテレメトリをリアルタイムで送信します。クリーンでシンプルなダッシュボードには、詳細なネットワークヘルスとフラグの問題が表示されます。次に、ガイド付き修復により解決が自動化され、日常的なトラブルシューティング作業が少なくなり、ネットワークのパフォーマンスが最適に保たれます。

その結果、一貫したエクスペリエンスとネットワークのプロアクティブな最適化が実現し、タスクのトラブルシューティングに費やす時間が短縮されます。

質問: 510

Firepower Next Generation Intrusion Prevention System検出器を、左側から右側の正しい定義にドラッグアンドドロップします。

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

正解:

PortScan Detection	Distributed PortScan
Port Sweep	Decoy PortScan
Decoy PortScan	Port Sweep
Distributed PortScan	PortScan Detection

質問: 511

WCCPでTCPトラフィックをリダイレクトするには、CiscoWSAでどのプロキシモードを使用する必要がありますか。

- A. 透明
- B. リダイレクト
- C. 転送
- D. プロキシゲートウェイ

正解: (正解を表示します)

説明CiscoWSAへのトラフィックのリダイレクトを実行するには、透過プロキシモードと明示プロキシモードの2つの方法があります。透過プロキシ展開では、WCCP v2対応ネットワークデバイスは、クライアントで設定を行わなくても、宛先がポート80または443のすべてのTCPトラフィックをCiscoWSAにリダイレクトします。この設計では透過プロキシ展開が使用され、すべてのアウトバウンドWebトラフィックがデバイスを通り、通常はCisco WSAを管理する同じ運用スタッフによって管理されるため、CiscoASAファイアウォールを使用してトラフィックをアプライアンスにリダイレクトします。参照 <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf>

Cisco WSAへのトラフィックのリダイレクトを実行するには、次の2つの方法があります。

透過プロキシ展開では、WCCP v2対応ネットワークデバイスは、クライアントで設定を行わなくても、宛先がポート80または443のすべてのTCPトラフィックをCiscoWSAにリダイレクトします。この設計では透過プロキシ展開が使用され、すべてのアウトバウンドWebトラフィックがデバイスを通り、通常はCisco WSAを管理する同じ運用スタッフによって管理されるため、CiscoASAファイアウォールを使用してトラフィックをアプライアンスにリダイレクトします。

説明CiscoWSAへのトラフィックのリダイレクトを実行するには、透過プロキシモードと明示プロキシモードの2つの方法があります。透過プロキシ展開では、WCCP v2対応ネットワークデバイスは、クライアントで設定を行わなくても、宛先がポート80または443のすべてのTCPトラフィックをCiscoWSAにリダイレクトします。この設計では透過プロキシ展開が使用され、すべてのアウトバウンドWebトラフィックがデバイスを通り、通常は

Cisco WSAを管理する同じ運用スタッフによって管理されるため、CiscoASAファイアウォールを使用してトラフィックをアプライアンスにリダイレクトします。参照 <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf>

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **512**

NetFlowを使用して、ネットワーク、データセンター、ブランチオフィス、およびクラウド全体の可視性を提供するセキュリティソリューションはどれですか。

- A. Cisco Umbrella
- B. Cisco Stealthwatch
- C. Cisco CTA
- D. Cisco Encrypted Traffic Analytics

正解: ([正解を表示します](#))

質問: **513**

管理者は、ポート80および443を介してリダイレクトされたトラフィックを受信するようにCisco WSAを設定します。組織では、特定のWSA統合機能を備えたネットワークデバイスを設定して、トラフィックをWSAに送信し、要求をプロキシして可視性を高め、これをユーザーこれらの要件をサポートするには、Cisco WSAで何をする必要がありますか？

- A. CiscoWSAおよびネットワークデバイスでWPADを使用してアクティブなトラフィックリダイレクトを設定します
- B. Cisco WSAのレイヤ4設定を使用して、ネットワークデバイスから明示的な転送要求を受信します
- C. CiscoWSAおよびネットワークデバイスでWCCPを使用して透過的なトラフィックリダイレクトを構成します
- D. PACキーを使用して、必要なネットワークデバイスのみがトラフィックをCiscoWSAに送信できるようにします。

正解: ([正解を表示します](#))

質問: **514**

展示を参照してください。

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
description Uplink_To_Distro_Switch_g1/0/1
switchport trunk native vlan 999
switchport trunk allowed vlan 40,41,44
switchport mode trunk
```

組織は、ネットワーク内でDHCPスヌーピングを使用しています。新しいスイッチのVLAN41のユーザーが、IPアドレスが取得されていないと不満を言っています。ユーザーにネットワーク接続を提供するために、スイッチインターフェイスでどのコマンドを設定する必要がありますか？

- A. ip dhcp snooping verify mac-address
- B. ip dhcp snooping limit 41
- C. ip dhcp snooping vlan 41
- D. ip dhcp snooping trust

正解: [\(正解を表示します\)](#)

参照 :

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html>

質問: 515

組織はネットワークセキュリティにCiscoFirepowerとCiscoMerakiMXを使用しており、これらのプラットフォーム全体でクラウドポリシーを一元管理する必要があります。この目標を達成するには、どのソフトウェアを使用する必要がありますか？

- A. Cisco Secureworks
- B. Cisco DNA Center
- C. Cisco Defense Orchestrator
- D. Cisco Configuration Professional

正解: [\(正解を表示します\)](#)

質問: 516

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

正解:

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

uses six packets in main mode to establish phase 1

uses three packets in aggressive mode to establish phase 1

IKEv2

standard includes NAT-T

uses four packets to establish phase 1 and phase 2

uses EAP for authenticating remote access clients

質問: 517

CiscoFirepowerがCiscoTalosから脅威インテリジェンスアップデートをダウンロードするタイミングを表す用語はどれですか。

- A. 共有
- B. オーサリング
- C. 分析
- D. 消費

正解: ([正解を表示します](#))

質問: 518

エンドポイントにインストールされた場合のCiscoUmbrellaRoamingの役割は何ですか？

- A. 企業ネットワークへの安全なVPN接続を確立する
- B. 姿勢コンプライアンスと必須ソフトウェアを適用する
- C. 悪意のあるファイル転送からエンドポイントを保護するため
- D. 企業ネットワークの内外の悪意のあるリンクから資産を保護するため

正解: D ([コメントを発表する](#))

質問: 519

マルチベンダー環境をサポートし、サイト間のトラフィックを保護できるVPNテクノロジーはどれですか？

- A. FlexVPN
- B. VPNを取得
- C. SSL VPN
- D. DMVPN

正解: A ([コメントを発表する](#))

質問: 520

Cisco ESAネットワーク管理者は、新しくインストールされたサービスを使用して、レピュテーション判定に基づいたポリシーの作成を支援するように任命されています。テスト中に、CiscoESAが未決定の評決を持つファイルをドロップしていないことがわかりました。この問題の原因は何ですか？

- A. ポリシーは、ドロップではなく隔離にメッセージを送信するために作成されました
- B. ファイルのレピュテーションスコアがしきい値を超えています
- C. ファイルのレピュテーションスコアがしきい値を下回っています
- D. ファイル分析を無効にするポリシーが作成されました

正解: ([正解を表示します](#))

説明

ESAと一緒に使用できる高度なマルウェア保護 (AMP)に関するこのQmentionsの「新しくインストールされたサービス」かもしれません。AMPは、攻撃の連続体全体で優れた保護を可能にします。

+ファイルレピュテーション-ESAを通過するときに各ファイルのフィンガープリントをキャプチャし、レピュテーション判定のためにAMPのクラウドベースのインテリジェンスネットワークに送信します。これらの結果があれば、悪意のあるファイルを自動的にブロックし、管理者が定義したポリシーを適用できます。

+ファイル分析-ESAを通過している未知のファイルを分析する機能を提供します。高度に安全なサンドボックス環境により、AMPはファイルの動作に関する正確な詳細を収集し、そのデータを詳細な人間およびマシンの分析と組み合わせて、ファイルの脅威レベルを判断できます。次に、この処理はAMP

クラウドベースのインテリジェンスネットワークに送られ、AMPクラウドデータセットを動的に更新および拡張して保護を強化するために使用されます。

質問: 521

ステップを左から右の正しい順序にドラッグアンドドロップして、AppDynamicsがアマゾンウェブサービスのEC2インスタンスを監視できるようにします。

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

正解:

Install monitoring extension for AWS EC2.	Install monitoring extension for AWS EC2.
Restart the Machine Agent.	Configure a Machine Agent or SIM Agent.
Update config.yaml.	Update config.yaml.
Configure a Machine Agent or SIM Agent.	Restart the Machine Agent.

質問: 522

CiscoASDMよりもCiscoFMCを使用する利点は何ですか。

- A. Cisco FMCはJavaを使用し、CiscoASDMはHTML5を使用します。
- B. Cisco FMCは集中管理を提供しますが、CiscoASDMは提供しません。
- C. Cisco FMCはデバイスへの設定のプッシュをサポートしていますが、CiscoASDMはサポートしていません。
- D. Cisco FMCはすべてのファイアウォール製品をサポートしますが、CiscoASDMはCiscoASAデバイスのみをサポートします

正解: (正解を表示します)

参照 :

<https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>

質問: 523

展示を参照してください。

```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
DEFAULT in the outbound table
```

どのタイプの認証が使用されていますか？

- A. MicrosoftOutlookのLDAP認証
- B. POP3認証
- C. SMTPリレーサーバー認証
- D. 外部ユーザーとリレーメール認証

正解: D (コメントを发表する)

TLS接続は、フィルターアクション、ウイルス対策およびスパム対策の判定、配信の試行など、メッセージに関連するその他の重要なアクションとともに、メールログに記録されます。TLS接続が成功すると、メールログにTLS成功エントリが記録されます。同様に、TLS接続に失敗すると、TLS失敗エントリが生成されます。メッセージのログファイルにTLSエントリが関連付けられていない場合、そのメッセージはTLS接続を介して配信されませんでした。

TLS接続は、フィルターアクション、ウイルス対策およびスパム対策の判定、配信の試行など、メッセージに関連するその他の重要なアクションとともに、メールログに記録されます。TLS接続が成功すると、メールログにTLS成功エントリが記録されます。同様に、TLS接続に失敗すると、TLS失敗エントリが生成されます。メッセージのログファイルにTLSエントリが関連付けられていない場合、そのメッセージはTLS接続を介して配信されませんでした。

参照：
このQの展示では、メールログにリモートホスト（受信からのTLS接続が成功したことが示されています。
TLS接続は、フィルターアクション、ウイルス対策およびスパム対策の判定、配信の試行など、メッセージに関連するその他の重要なアクションとともに、メールログに記録されます。TLS接続が成功すると、メールログにTLS成功エントリが記録されます。同様に、TLS接続に失敗すると、TLS失敗エントリが生成されます。メッセージのログファイルにTLSエントリが関連付けられていない場合、そのメッセージはTLS接続を介して配信されませんでした。
このQの展示では、メールログにリモートホスト（受信からのTLS接続が成功したことが示されています。

質問: 524

説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

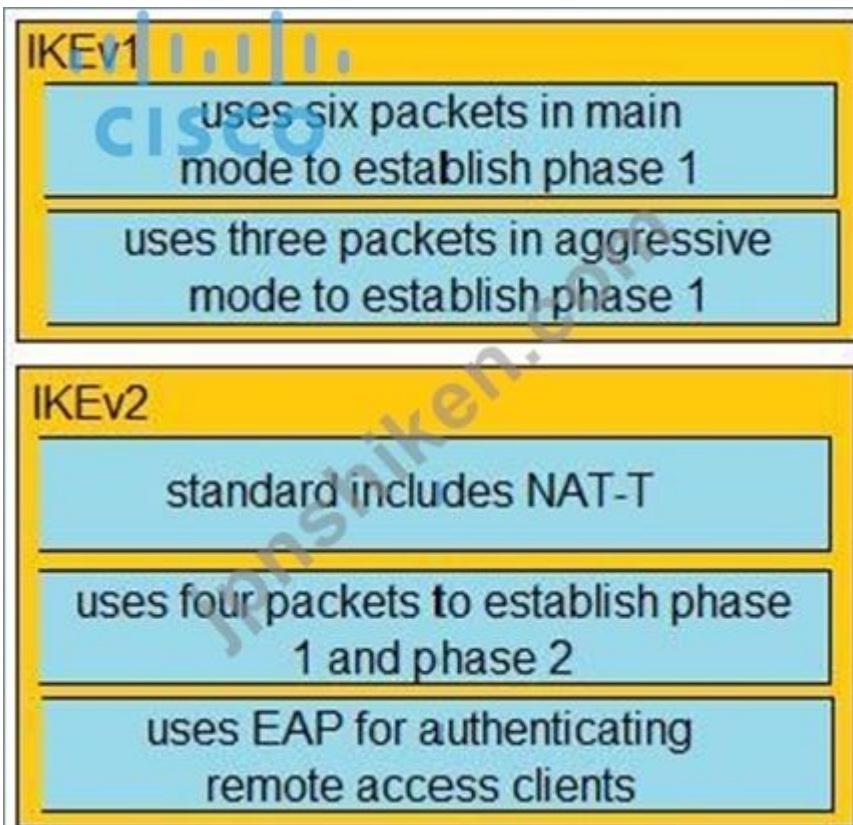
IKEv1

IKEv2

正解:



説明



質問: 525

コンテンツセキュリティに使用されるAPIはどれですか？

- A. AsyncOS API
- B. OpenVuln API
- C. IOS XR API
- D. NX-OS API

正解: **A** ([コメントを发表する](#))

質問: **526**

Cisco Firepower Next Generation Intrusion Prevention Systemのホスト情報をキャプチャするために使用されるポリシーはどれですか？

- A. 相関
- B. 侵入
- C. アクセス制御
- D. ネットワークディスカバリー

正解: ([正解を表示します](#))

説明Firepowerシステムは、ネットワーク検出およびIDポリシーを使用して、ネットワーク上のトラフィックのホスト、アプリケーション、およびユーザーデータを収集します。特定の種類の検出およびIDデータを使用して、ネットワーク資産の包括的なマップを構築し、フォレンジック分析、動作プロファイリング、アクセス制御を実行し、組織が影響を受けやすい脆弱性とエクスプロイトを軽減および対応できます。ホストとアプリケーションの検出を実行するようにネットワーク検出ポリシーを構成できます。参照：

[https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html)

[v64/introduction_to_network_discovery_and_identity.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html) Firepowerシステムは、ネットワーク検出およびIDポリシーを使用しますネットワーク上のトラフィックのホスト、アプリケーション、およびユーザーデータを収集します。

ホストとアプリケーションの検出を実行するようにネットワーク検出ポリシーを構成できます。

説明Firepowerシステムは、ネットワーク検出およびIDポリシーを使用して、ネットワーク上のトラフィックのホスト、アプリケーション、およびユーザーデータを収集します。特定の種類の検出およびIDデータを使用して、ネットワーク資産の包括的なマップを構築し、フォレンジック分析、動作プロファイリング、アクセス制御を実行し、組織が影響を受けやすい脆弱性とエクスプロイトを軽減および対応できます。ホストとアプリケーションの検出を実行するようにネットワーク検出ポリシーを構成できます。参照：

[https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html)

[v64/introduction_to_network_discovery_and_identity.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html)

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **527**

展示を参照してください。ネットワーク上でAAAセッションを行うことを可能にする構成アイテムはどれですか。

- A. aaa authentication login console ise
- B. aaa authentication enable default enable
- C. aaa authentication exec default ise
- D. AAA許可ネットワークのデフォルトグループise

正解: ([正解を表示します](#))

質問: **528**

概念を左から右の正しい説明にドラッグアンドドロップします

guest services	requires probes to collect attributes of connected endpoints
profiling	sponsor portal that is used to gain access to network resources
posture assessment	My Devices portal that allows users to register their device
BYOD	Results can have a status of compliant or noncompliant.

正解:

guest services	profiling
profiling	guest services
posture assessment	BYOD
BYOD	posture assessment

質問: 529

コグニティブ脅威分析の2つの検出および分析エンジンとは何ですか？ 2つ選択してください。）

- A. データの漏えい
- B. コマンドアンドコントロール通信
- C. インテリジェントプロキシ
- D. snort
- E. URLの分類

正解: A,B ([コメントを发表する](#))

説明/リファレンス <https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf>

質問: 530

どのパブリッククラウドプロバイダーがCiscoNextGeneration Firewall Virtualをサポートしていますか？

- A. Google Cloud Platform
- B. Red Hat Enterprise Visualization
- C. VMware ESXi
- D. アマゾンウェブサービス

正解: ([正解を表示します](#))

説明

Cisco Firepower NGFWv in Amazon Web Services (AWS) or Microsoft Azure must be managed by a Cisco Firepower Management Center (FMC) residing in AWS or on-premises. The virtual FCM can be deployed on VMware ESXi, on KVM, and in AWS. Figure 1 shows the various FMC dashboards.

質問: 531

欺瞞的なフィッシングとスパフィッシングの違いは何ですか？

- A. 詐欺的なフィッシングは、Cレベルの役割を持つ組織内の特定のユーザーを狙った攻撃です。
- B. スパフィッシングキャンペーンは、特定の個人とグループの人々を対象としています。
- C. スパフィッシングとは、攻撃が組織のCレベルの幹部を狙ったものです。
- D. 詐欺的なフィッシングは、被害者のDNSサーバーを乗っ取って操作し、ユーザーを偽のWebページにリダイレクトします。

正解: B ([コメントを发表する](#))

説明

詐欺的なフィッシングでは、詐欺師が合法的な企業になりすまして、人々の個人データやログイン資格情報を盗もうとします。これらの電子メールは、攻撃者が望むことを実行するようにユーザーを怖がらせるために、脅威と切迫感を頻繁に使用します。

スパフィッシングは、1人の受信者が応答するように注意深く設計されています。犯罪者は、ソーシャルメディアやその他の公開情報を使用して、組織内の個々のターゲットを選択し、その個人に合わせた偽の電子メールを作成します。

有効的な**350-701**問題集はJPNTTest.com提供され、**350-701**試験に合格することに役に立ちます！JPNTTest.comは今最新**350-701**試験問題集を提供します。JPNTTest.com 350-701試験問題集はもう更新されました。ここで**350-701**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/350-701-mondaishu> **727**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」