Cisco.350-701J.v2023-08-17.q268

試験コード：	350-701J
試験名称：	Implementing and Operating Cisco Security Core Technologies (350-701日本語版)
認証ベンダー：	Cisco
無料問題の数：	268
バージョン：	v2023-08-17
ページの閲覧量：	383
問題集の閲覧量：	18478

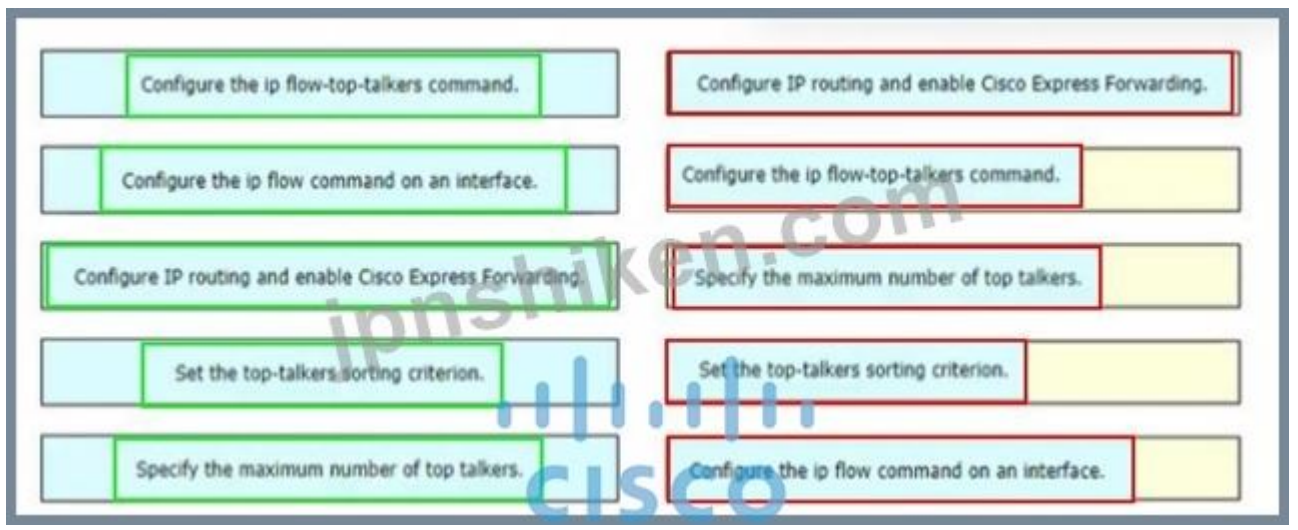
https://www.jpnshiken.com/shiken/Cisco.350-701J.v2023-08-17.q268.html

質問: **1**
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. aaa new-model
B. ipデバイス追跡
C. auth-type all
D. aaa server radius dynamic-author
正解: **(**正解を表示します**)**

質問: **2**
小規模な組織では、10.0.0.0 / 24ローカルHQネットワーク上の企業リソースにアクセスする必要があるVPNユーザーが帯域幅を利用できるようにするために、ヘッドエンドCiscoASAのVPN帯域幅の負荷を減らす必要があります。ネットワークにデバイスを追加せずに、これをどのように実現しますか？
A. 10.0.0.0/24ネットワークのトラフィックを分散するようにVPN負荷分散を構成します。
B. スプリットトンネリングを使用して、10.0.0.0/24ネットワークのトラフィックのみをトンネリングします。
C. 企業以外のトラフィックをインターネットに直接送信するようにVPN負荷分散を構成します。
D. スプリットトンネリングを使用して、10.0.0.0/24ネットワークを除くすべてのトラフィックをトンネリングします。
正解: **B (**コメントを発表する**)**

質問: **3**
ネットワーク エンジニアが Cisco ルータで NetFlow トップ トーカーを設定しています プロセスの手順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

正解:



質問: **4**
受信メールと送信メールを分離する ESA 実装方法はどれですか?
A. 論理 IPv4 リスナーのペアと IPv6 リスナーのペアが物理的に分離された 2 つのインターフェイスにある
B. 2 つの一意の論理 IPv4 アドレスと 1 つの IPv6 アドレスを持つ単一の物理インターフェイス上の論理リスナーのペア
C. 1 つの物理インターフェイス上の 1 つのリスナー
D. 1 つの論理インターフェイス上の 1 つの論理 IPv4 アドレスに 1 つのリスナー
正解: **(**正解を表示します**)**

質問: **5**
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. プット
B. オプション
C. 取得
D. プッシュ
E. 接続
正解: **A,C (**コメントを発表する**)**

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.
All API requests are sent over HTTPS to the ASA, and a response is returned.
Request Structure
Available request methods are:
GET - Retrieves data from the specified object.
PUT - Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.
POST - Creates the object with the supplied information.
DELETE - Deletes the specified object
PATCH - Applies partial modifications to the specified object.

質問: **6**
悪意のあるユーザーは、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ー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何ですか？ （2つ選択してください）
A. 802.1AE MacSec
B. ポートセキュリティ
C. プライベートVLAN
D. IPデバイストラック
E. DHCPスヌーピング
F. 動的ARP検査
正解: **E,F** (コメントを発表する)

質問: **7**
エンジニアはCisco Umbrella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Cisco Umbrellaネットワーク経由で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. インテリジェントプロキシが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できるようにします。
B. クライアントコンピューターが背後にあるパブリックIPアドレスをコアアイデンティティに追加します。
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検証します。
D. クライアントコンピューターがオンプレミスDNSサーバーを指していることを確認します。
正解: (正解を表示します)

質問: **8**
メッセンジャープロトコルの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ンジャーアプリケーションに感染して、企業データを送信します。
B. 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。
C. 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。
D. 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。
E. メッセンジャー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

正解: **(**正解を表示します**)**

質問: **9**
展示を参照してください。URLフィルタリングのアクセスルールを作成するとき、ネットワークエンジニアは、ブロックする特定のカテゴリと個々のURLを追加します。構成の結果は何ですか？
A. レピュテーションスコアが3のボットネットのURLのみが許可され、残りはブロックされます。
B. レピュテーションスコアが1～3のボットネットのURLのみがブロックされます。
C. レピュテーションスコアが3のボットネットのURLのみがブロックされます。
D. レピュテーションスコアが3～5のボットネットのURLのみがブロックされます。
正解: **(**正解を表示します**)**

質問: **10**
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. ファイルレピュテーションセンター
B. AMPレピュテーションセンター
C. IPスロックリストセンター
D. IPおよびドメインレピュテーションセンター
正解: **D (**コメントを発表する**)**

質問: **11**
データセキュリティのためのCisco Cloudlockの機能は何ですか？
A. 悪意のあるクラウドアプリを制御します
B. データ損失防止
C. ユーザーとエンティティの行動分析
D. 異常を検出します
正解: **B (**コメントを発表する**)**

質問: **12**
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**)**
The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?). In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. Reference:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/ security-overview.html (The data plane is also sometimes called the forwarding plane.) Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?).
In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates.
The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?). In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. Reference:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/ security-overview.html

質問**: 13**
Cisco電子メールセキュリティアプライアンスの主な役割は何ですか？
A. メール送信エージェント
B. メール転送エージェント
C. メール配信エージェント
D. メールユーザーエージェント
正解**: (**正解を表示します**)**
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.
Reference:
Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

質問**: 14**
Cisco Firepower Management Centerで、管理対象デバイスからヘルスモジュールアラートを収集するために使用されるポリシーはどれですか。
A. 健康政策
B. システムポリシー
C. アクセス制御ポリシー
D. 健康意識の方針
E. 相関ポリシー
正解**: (**正解を表示します**)**

質問**: 15**
Cisco AMPforEndpointsとCiscoUmbrellaの違いは何ですか。
A. Cisco AMP for Endpointsはクラウドベースのサービスですが、CiscoUmbrellaはそうではありません。

B. Cisco AMP for Endpointsは、悪意のある宛先への接続やCマルウェアを防ぎます。
C. Cisco AMP for Endpointsは、侵入の痕跡を自動的に調査します。
D. Cisco AMP for Endpointsは、インターネットの脅威の前および脅威に対する攻撃を防止、検出、および対応します。
正解: **(**正解を表示します**)**
https://learn-umbrella.cisco.com/i/802005-umbrella-security-report/3?
https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Powerful%20EDR%20capabilities,from%20Kenna%20Security.
Cisco Advanced Malware Protection (AMP) for endpoints can be seen as a replacement for the traditional antivirus solution. It is a next generation, cloud delivered endpoint protection platform (EPP), and advanced endpoint detection and response (EDR). Providing Protection - Detection Response While Cisco Umbrella can enforce security at the DNS-, IP-, and HTTP/S-layer, this report does not require that blocking is enabled and only monitors your DNS activity. Any malicious domains requested and IPs resolved are indicators of compromise (IOC).
Any malicious domains requested and IPs resolved are indicators of compromise (IOC)

質問: **16**
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
正解: **C (**コメントを発表する**)**
In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.

質問: **17**
脆弱性とエクスプロイトの違いは何ですか？
A. エクスプロイトは、ネットワークに脆弱性を引き起こす架空のイベントです
B. 脆弱性は、攻撃者が悪用する架空のイベントです

C. エクスプロイトは、ネットワークに脆弱性を引き起こす可能性のある弱点です
D. 脆弱性は、攻撃者が悪用できる弱点です。
正解: **(**正解を表示します**)**

質問: **18**
エンドポイント保護エンドポイント検出と応答の組み合わせを提供するテクノロジーはどれですか？
A. Cisco Umbrella
B. Cisco AMP
C. Cisco Threat Grid
D. Cisco Talos
正解: **(**正解を表示します**)**

質問: **19**
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 noauth
asa-host（config）#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX 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 3des ciscXXXXXXXX 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 aes 256 ciscXXXXXXXX asa-host（config）#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host（config）#snmp-server group myv3 v3 priv
asa-host（config）#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX 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: **20**
不足しているパッチの検出と修復に役立つ Cisco ISE 機能はどれですか?
A. プロファイリング ポリシー
B. 姿勢評価
C. プローブを有効にする
D. 認証ポリシー
正解: **(**正解を表示します**)**

質問: **21**
ネットワークエンジニアがCiscoASAにNTPサーバを設定しました。Cisco ASAは、NTPサーバへのIP到達可能性を備えており、トラフィックをフィルタリングしていません。show ntpassociation detailコマンドは、設定されたNTPサーバが同期されておらず、ストラタムが16であることを示しています。

この問題の原因は何ですか？
A. 内部インターフェイスのUDPポート123のアクセスリストエントリがありません。
B. NTPは稼働中のサーバーを使用するように構成されていません。
C. NTPの再同期は強制されません
D. 外部インターフェイスのUDPポート123のアクセスリストエントリがありません。
正解: **B** (コメントを発表する)

質問: **22**
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)
Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:
+ Ingress interface (SNMP ifIndex)
+ Source IP address
+ Destination IP address
+ IP protocol
+ Source port for UDP or TCP, 0 for other protocols
+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
+ IP Type of Service
Note: A flow is a unidirectional series of packets between a given source and destination.

質問: **23**
ユーザーがアクセスできないようにマシンまたはネットワークをシャットダウンしようとする攻撃タイプはどれですか？
A. smurf
B. bluesnarfing
C. MAC spoofing
D. IP spoofing
正解: **A** (コメントを発表する)
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to its intended users.
The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

質問: **24**
ネイティブ API を使用してデバイスを Cisco DNA Center に追加するには、どの API メソッドと必須属性を使用しますか?
A. GET とシリアル番号

B. userSudiSerlalNos および deviceInfo
C. lastSyncTime と pid
D. POST と名前
正解: **(**正解を表示します**)**

質問: **25**
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. ESAはインラインで展開されます
B. 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。
C. 需要は予測できません
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 (**コメントを発表する**)**

質問: **26**
Cisco Cognitive Threat Analytics を使用して、危険なサイトを自動的にブロックし、ユーザーがクリックできるようにする前に未知のサイトに隠された高度な脅威をテストするプラットフォームはどれですか?
A. Cisco Advanced Stealthwatch Appliance (ASA)
B. Cisco Web Security Appliance (WSA)
C. Cisco Identity Services Engine (ISE)
D. Cisco Enterprise Security Appliance (ESA)
正解: **(**正解を表示します**)**

質問: **27**
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. Cisco Endpoint Security Analytics
C. セキュリティ姿勢評価サービス
D. エンドポイント向けCisco AMP
正解: **(**正解を表示します**)**

質問: **28**
デバイスコンプライアンスを実行する利点は何ですか？
A. 最新のOSパッチの検証
B. デバイスの分類と承認
C. 多要素認証の提供
D. 属性駆動型ポリシーの提供
正解: **(**正解を表示します**)**

質問: **29**

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. Cisco DNA Center API呼び出しを利用するには、Postmanが必要です。
B. ネットワークの全体的な状態を表示します
C. これらはシスコ独自のものです。
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. Pythonスクリプトをサポートしていません。
正解: **(**正解を表示します**)**

質問: **30**
Cisco AMP for Endpoints の機能は何ですか?
A. Web ベースの攻撃から保護します
B. 感染したホストの脅威への対応を自動化します
C. メールベースの攻撃をブロックします
D. DNS 攻撃を検出します
正解: **(**正解を表示します**)**

質問: **31**
断片化されたパケットを使用して標的のマシンをクラッシュさせようとする DoS 攻撃はどれですか?
A. ティアドロップ
B. ランド
C. SYNフラッド
D. スマーフ
正解: **(**正解を表示します**)**

質問: **32**
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. IPレピュテーションフィルタリング
B. インテリジェントマルチスキャン
C. アンチウイルスフィルタリング
D. ファイル分析
正解: **B (**コメントを発表する**)**

質問: **33**
WSAがアプリケーショントラフィックを復号化するために証明書を使用する前に、証明書が満たす必要がある2つの基準はどれですか。（2つ選択してください。）
A. 現在の日付を含める必要があります。
B. SANが含まれている必要があります。
C. 内部CAによって署名されている必要があります。
D. WSAの信頼できるストアに存在する必要があります。
E. エンドポイントのトラステッドストアに存在する必要があります。
正解: **(**正解を表示します**)**

質問: **34**
Cisco ASA FirePOWERモジュールがサポートする2つの展開モードはどれですか。（2つ選択してください。）
A. 透過モード
B. ルーテッドモード
C. インラインモード
D. アクティブモード
E. パッシブモニター専用モード
正解: **(**正解を表示します**)**
You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference:
modules-sfr.html

質問: **35**
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化方法ですか？
A. 3DES
B. RSA
C. DES
D. AES
正解: **(**正解を表示します**)**
Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

質問: **36**
ネットワークエンジニアがDMVPNを設定していて、ホストAでcrypto isakmp key cisc0380739941 address0.0.0.0コマンドを入力しました。hostB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. hostBで別のパスワードを使用してコマンドを入力します。
B. hostA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. hostBで同じコマンドを入力します。
D. hostAのコマンドでisakmpをikev2に変更します。

正解: **(**正解を表示します**)**

質問: **37**
Cisco DNACenter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: **(**正解を表示します**)**
Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-so-cte-en.html Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.
Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints,

and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.
Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.
The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups.
Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.
The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks.
Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-so-cte-en.html

質問**: 38**
ネットワーク テレメトリで最も一般的に使用されているプロトコルは何ですか?
A. NctFlow
B. TFTP
C. SNMP

D. SMTP
正解: **(**正解を表示します**)**

質問: **39**
サーバーに新しい証明書を追加するときの証明書署名要求の目的は何ですか？
A. インストールに必要な証明書のパスワードです。
B. サーバー情報を提供するため、証明書を作成して署名できます
C. サーバーがインストール時に認証できるように、証明書クライアント情報を提供します
D. サーバーにロードされるのは証明書です
正解: **(**正解を表示します**)**
A certificate signing request (CSR) is one of the first steps towards getting your own SSL Certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) that the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key

質問: **40**
Cisco Firepower Next Generation Intrusion Prevention Systemでネットワークディスカバリポリシーが必要な機能はどれですか。
A. セキュリティインテリジェンス
B. ヘルスモニタリング
C. URLフィルタリング
D. 影響フラグ
正解: **(**正解を表示します**)**

質問: **41**
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. SYNフラッド
C. ファーミング
D. スローロリス
正解: **(**正解を表示します**)**

質問: **42**
DevSecOpsプロセスの属性は何ですか？
A. 義務付けられたセキュリティ管理とチェックリスト
B. セキュリティスキャンと理論上の脆弱性
C. 開発セキュリティ
D. 孤立したセキュリティチーム
正解: **(**正解を表示します**)**

DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives.
Three key things make a real DevSecOps environment:
+ Security testing is done by the development team.
+ Issues found during that testing is managed by the development team.
+ Fixing those issues stays within the development team.

質問: **43**
Cisco ASA Netflowの機能は何ですか？
A. 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
B. MPFが設定されていなくてもNSELイベントを生成します
C. 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
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: **A** (コメントを発表する)
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01101.html
Policy Order The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed. If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

質問: **44**
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プ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: **A** (コメントを発表する)
As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles. Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP

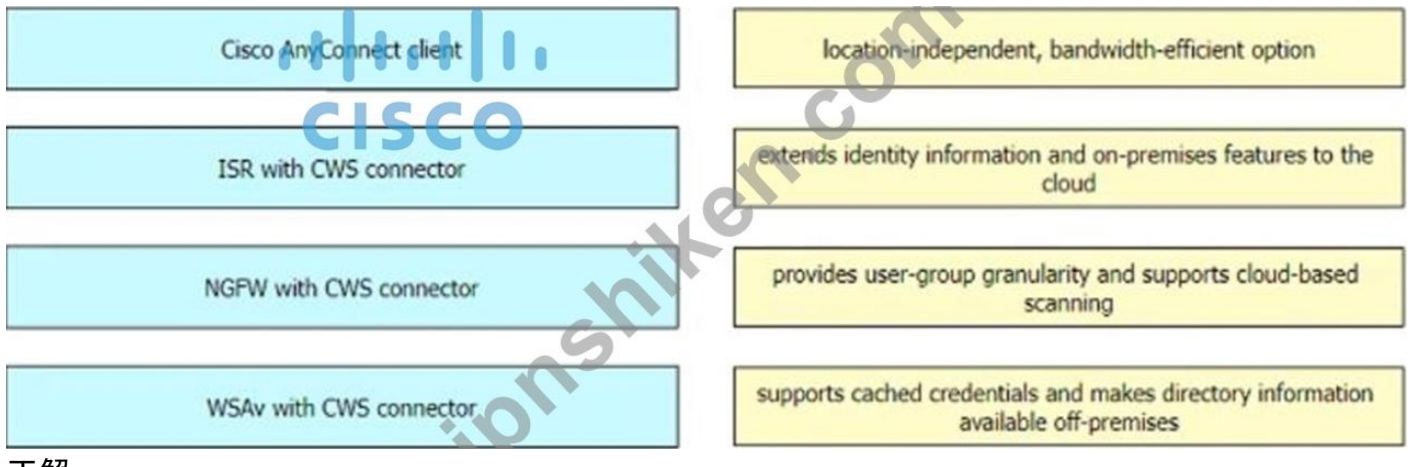
phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone. Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456 MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.
Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone.
As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles. Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone. Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

質問**: 45**
組織は、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は、ファイアウォールを介したアクセスをブロックする必要があります。これには、管理者が、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. 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
B. 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はそうではありません。

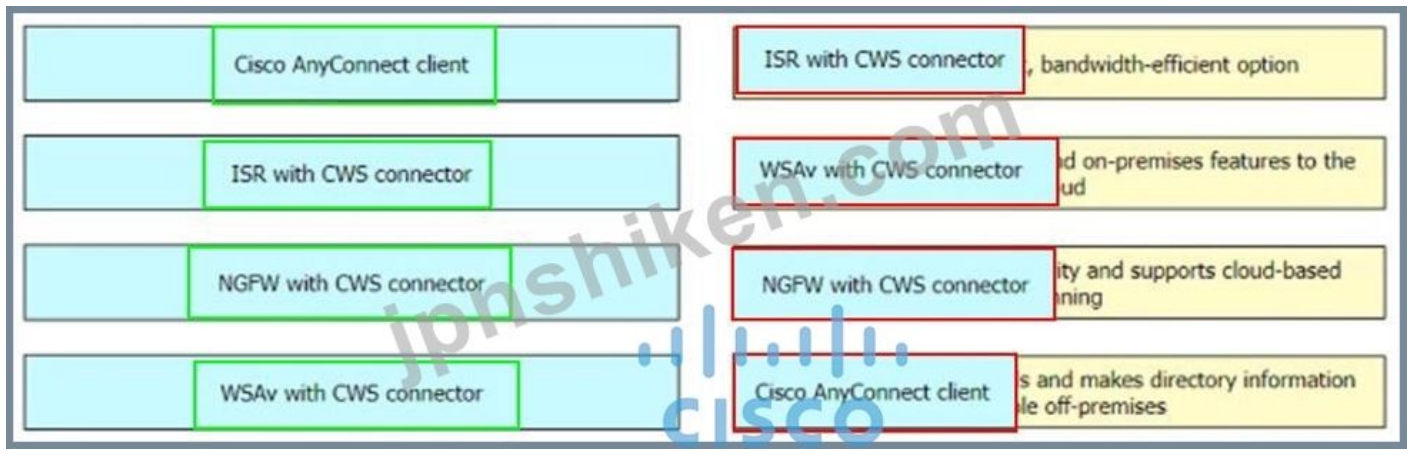
C. アクセス制御ポリシー機能にURLフィルタリングが含まれているため、Cisco ASAは含まれていますが、CiscoFTDには含まれていません。
D. Cisco FTDは、デフォルトでURLフィルタリングを有効にし、悪意のあるURLをブロックしますが、CiscoASAはそうではありません。
正解: **(**正解を表示します**)**

質問: **46**
資料を参照してください Cisco FMC でこのアクセス コントロール ルールを設定する場合、設定が展開されると、DMZjnside ゾーン宛てのトラフィックはどうなりますか?
A. すでに信頼されていない限り、DMZ_inside ゾーンへのトラフィックは許可されません。
B. 任意のゾーンからのすべてのトラフィックは、検査後にのみ DMZ_inside ゾーンに許可されます
C. 任意のゾーンから DMZ_inside ゾーンへのすべてのトラフィックは、それ以上の検査なしで許可されます
D. 信頼されているかどうかに関係なく、DMZ_inside ゾーンへのトラフィックは許可されません。
正解: **(**正解を表示します**)**

質問: **47**
Cisco CWS リダイレクション オプションを左側から右側の機能にドラッグ アンド ドロップします。



正解:



質問: 48

展示を参照してください。

Cisco ASA REST API の Python スクリプト コード スニペットの機能は何ですか?

A. Cisco ASA ファイアウォールの保存された構成を取得します。

B. ポリシーにグローバル ルールを追加します。

C. ポリシーからグローバル ルールを削除します。

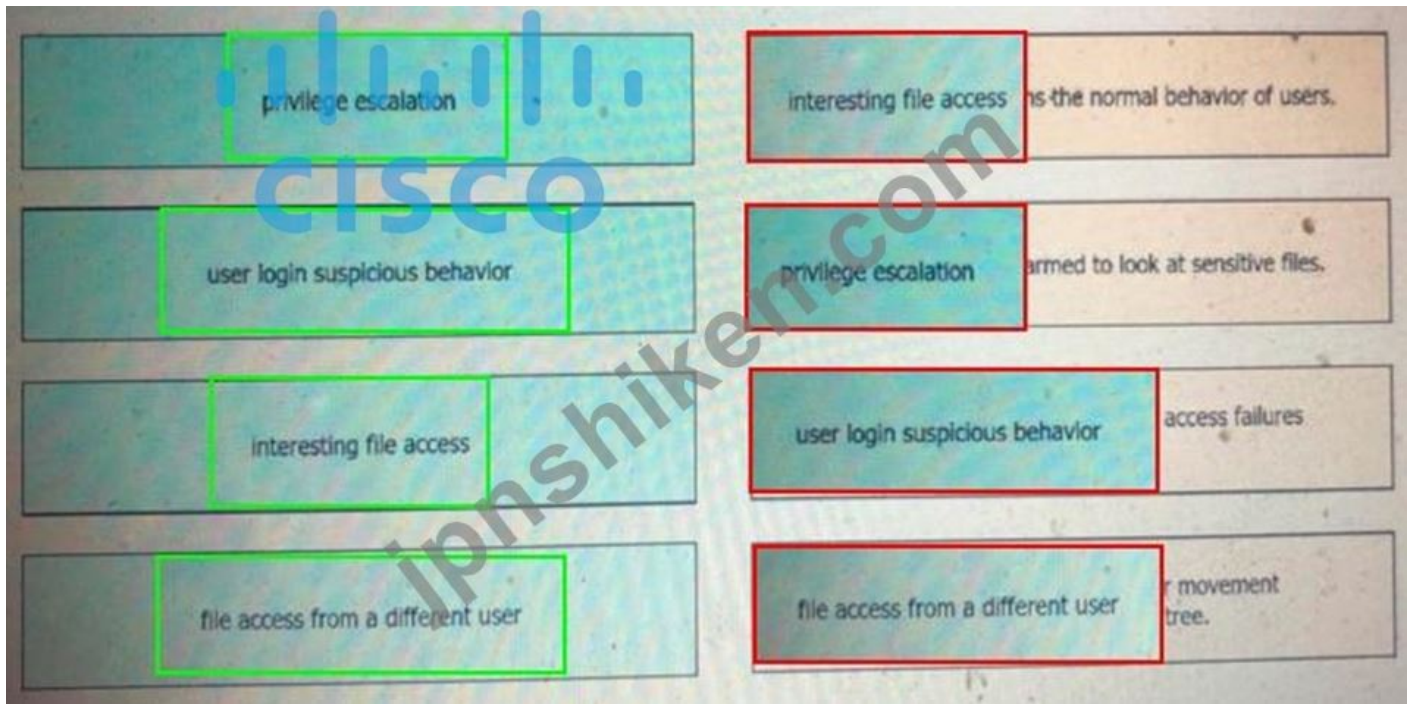
D. Cisco ASA のホスト名を変更します。

正解: **B** (コメントを発表する)

質問: **49**
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. 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**)**
Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.
The Zero Trust model uses microsegmentation - a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network - to contain attacks.

質問: **50**
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: **51**
IKEv1 にはあるが IKEv2 にはない 2 つの機能は? (2つ選んでください)
A. IKEv1 では、モードはメイン モードよりも高速にネゴシエートします。
B. NAT-T は IKEv1 でサポートされていますが、IKEv2 では無効です。
C. IKEv1 では、アグレッシブ モードを使用すると、イニシエーターとレスポンダーの ID がクリアテキストで渡されます。
D. IKEv1 は EAP 認証を使用します
E. IKEv1 会話は IKE_SA_INIT メッセージによって開始されます
正解: **(**正解を表示します**)**

質問: **52**
特定のグループの複数の組織がインフラストラクチャを共有し、共同でアクセスする共同作業であるクラウドモデルはどれですか？
A. ハイブリッド
B. コミュニティ
C. プライベート
D. 公開
正解: **(**正解を表示します**)**
Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party.

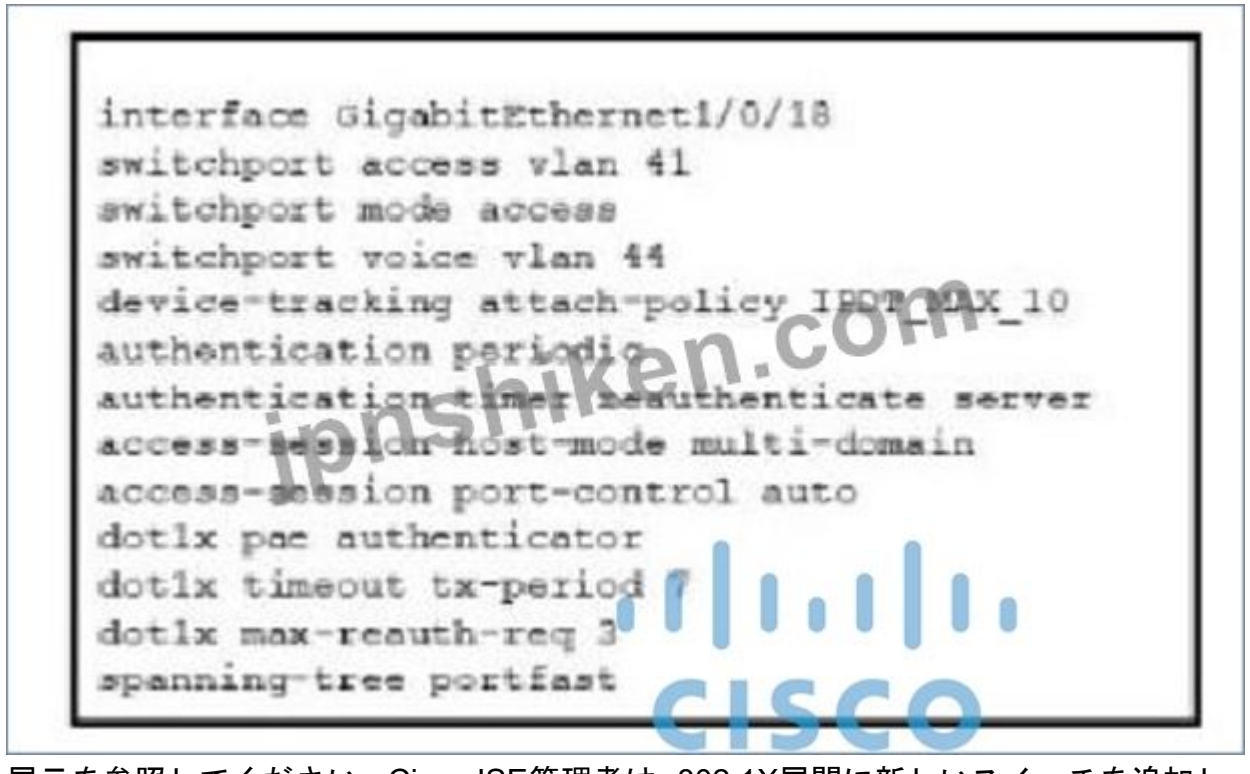
質問: **53**
企業は、オンプレミスに保存されていないクレジットカード番号の流出を経験しています。企業は、環境全体で機密データを保護できる必要があります。この目標を達成するには、どのツールを使用する必要がありますか？
A. セキュリティマネージャー
B. クラウドロック
C. Webセキュリティアプライアンス

D. Cisco ISE
正解: **(**正解を表示します**)**
Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

質問: **54**
BYOD用に設定する必要がある2つのCiscoISEコンポーネントはどれですか。（2つ選択してください。）
A. local WebAuth
B. null WebAuth
C. central WebAuth
D. dual
E. guest
正解: **C,E (**コメントを発表する**)**

質問: **55**
エンジニアが Cisco Umbrella 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。ID が使用する必要があるポリシーが 2 番目のポリシー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. タイムスタンプが最後に変更されたポリシーのみを構成します。
B. 最も具体的な構成を持つポリシーをポリシーの順序の最後に配置します
C. 要求を正しいポリシーにリダイレクトするように既定のポリシーを構成します。
D. ポリシーの順序で正しいポリシーを最初に作成します。
正解: **(**正解を表示します**)**

質問: **56**
展示を参照してください。



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CiscoISE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. 許可されたプロトコル構成でCiscoISE内の安全でないプロトコルを有効にします。
B. インターフェース構成にmabを追加します。
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. 認証イベントの構成失敗再試行2アクションインターフェイスでVLAN41を承認します
正解: **B** (コメントを発表する)

質問: **57**
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 Identity ServicesEngineでポスチャポリシーを設定します。
B. Cisco Identity Service Engineでプロファイリングポリシーを設定して、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します。
C. 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ように、Cisco Identity ServicesEngine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。
E. エンドポイントに重大な脆弱性がタイムリーにパッチされるように、明確に定義されたエンドポイントパッチ戦略を設定します

正解: (正解を表示します)
A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.
In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware.

質問: **58**
攻撃者は、ターゲットシステムにアクセスできるように、ターゲットシステムで偵察を実行する必要があります。システムのパスワードが弱く、VPNリンクが暗号化されておらず、システムのアプリケーションにソフトウェアのバグがあります。攻撃者がパスワードがクリアテキストで送信されていることを確認できる脆弱性はどれですか？
A. 認証用の弱いパスワード
B. トラフィックの暗号化されていないリンク
C. アプリケーションのソフトウェアバグ
D. 不適切なファイルセキュリティ

正解: **(**正解を表示します**)**

質問: **59**
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. ネットワーク検出
正解: **D (**コメントを発表する**)**
The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. You can configure your network discovery policy to perform host and application detection.

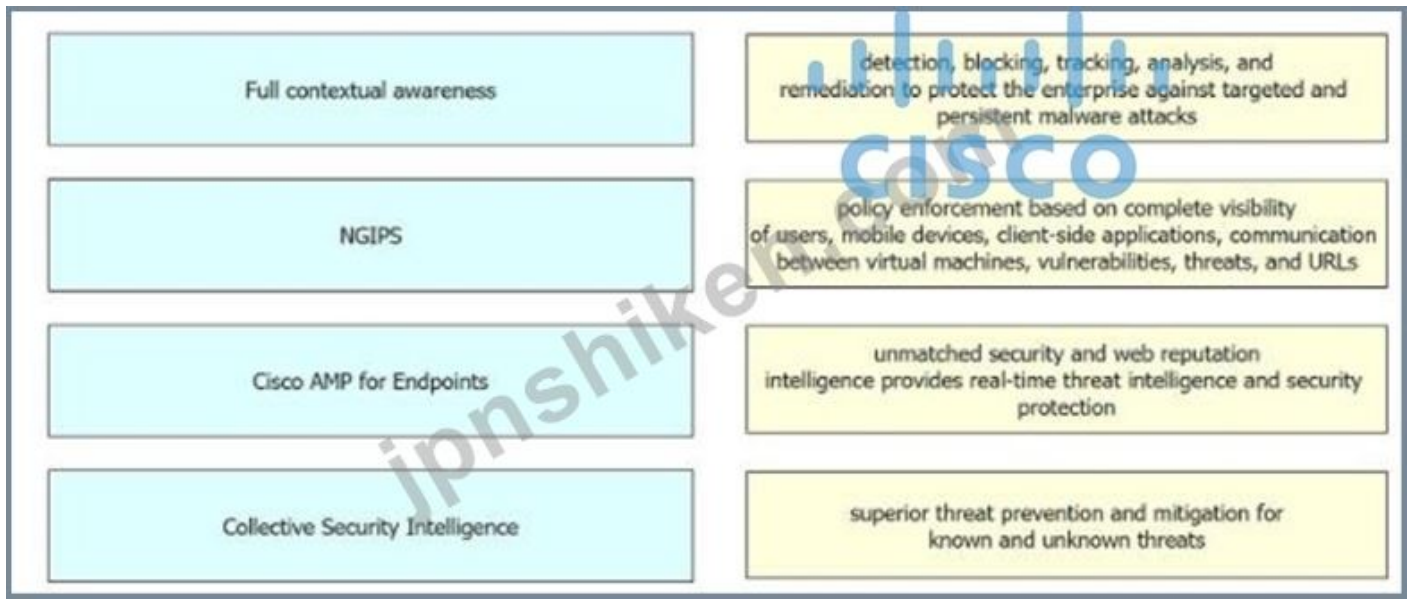
質問: **60**
VPNのセキュアハッシュアルゴリズムによって何が提供されますか？
A. 整合性
B. 鍵交換
C. 暗号化
D. 認証
正解: **(**正解を表示します**)**
The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMAC-SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404.

質問: **61**
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Amazon WebServicesのEC2インスタンスを監視できるようにします。

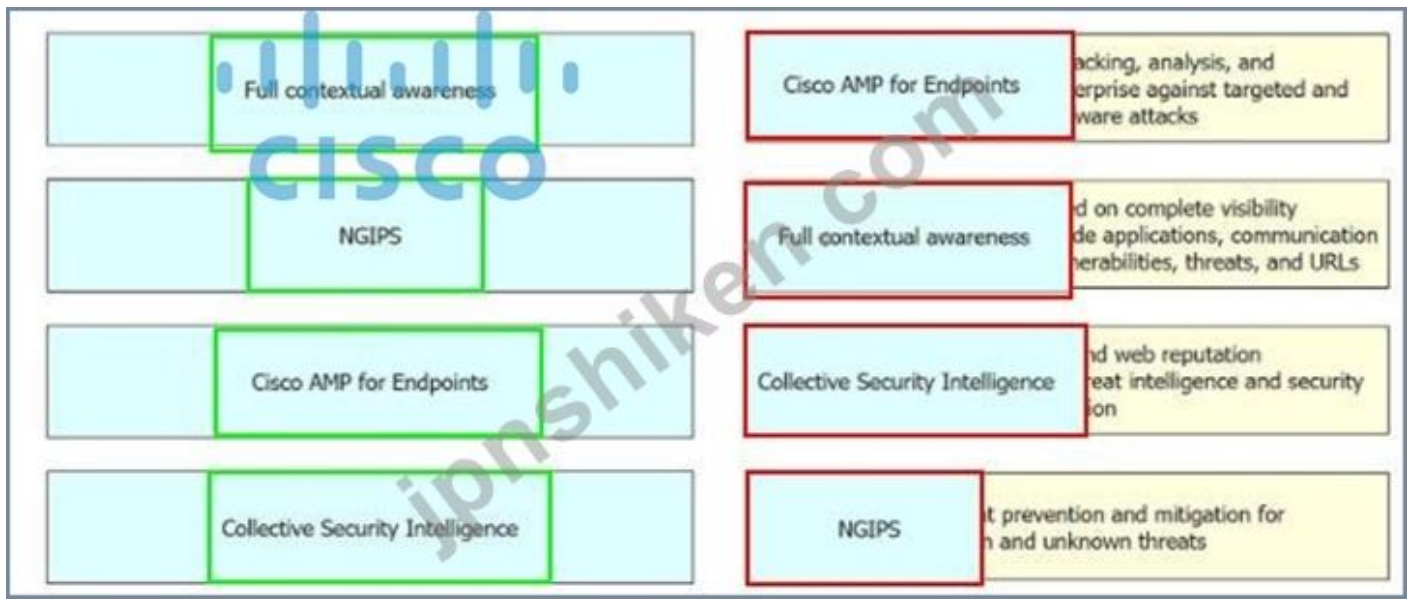
正解:

質問: **62**
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. スケーラビリティ
B. セキュリティ
C. カプセル化
D. 精度
正解: (正解を表示します)

質問: **63**
セキュリティソリューションを左側から右側に提供するメリットにドラッグアンドドロップします。



正解:



質問: **64**
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、CiscoISE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 allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Reference:
b_ise_admin_guide_sample_chapter_010101.html

質問: **65**
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カバリー
D. アクセス制御
正解: **A (**コメントを発表する**)**
NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the metadata for communications. It is a standard form of session data that details who, what, when, and where of network traffic -> Answer A is not correct.
Reference:

white-paper-c11-736595.html

質問: **66**
ゾーン定義が必要な Cisco Firewall ソリューションはどれですか?
A. ZBFW
B. CBAC
C. Cisco AMP
D. Cisco ASA
正解: **(**正解を表示します**)**

質問: **67**
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. 透過的なユーザーID
B. SOCKSプロキシサービス
C. Web使用制御
D. ユーザーセッションの制限
正解: **(**正解を表示します**)**

質問: **68**
マイクロセグメンテーションの説明は何ですか？
A. 環境は、Kubernetesなどのコンテナオーケストレーションプラットフォームをデプロイして、アプリケーションの配信を管理します
B. 環境はゼロトラストモデルを適用し、さまざまなサーバーまたはコンテナー上のアプリケーションが通信する方法を指定します
C. 環境は、同様のアプリケーションでサーバーをグループ化するためにプライベートVLANセグメンテーションを実装します。
D. 環境は、集中管理されたホストベースのファイアウォールルールを各サーバーまたはコンテナーに展開します
正解: **(**正解を表示します**)**

質問: **69**
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**)**
A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's alloted memory space. This happens quite frequently in the case of arrays.

質問: **70**

コンプライアンスチェックとリモートワイプを実行するシステムはどれですか？
A. MDM
B. AMP
C. OTP
D. ISE
正解: **(**正解を表示します**)**

質問: **71**
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. 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します
B. プロキシ自動設定ファイルを参照する
C. 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
D. Webキャッシュ通信プロトコルを使用する
E. 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
正解: **(**正解を表示します**)**

質問: **72**
フィッシング攻撃からユーザーを保護する際のエンドポイントの役割は何ですか？
A. 802.1Xネットワークセキュリティを利用して、リソースへの不正アクセスを保証します。
B. 機械学習モデルを使用して、異常を特定し、予想される送信動作を判断します。
C. CiscoStealthwatchとCiscoISEIntegrationを使用します。
D. ウイルス対策およびマルウェア対策ソフトウェアが最新であることを確認します。
正解: **(**正解を表示します**)**

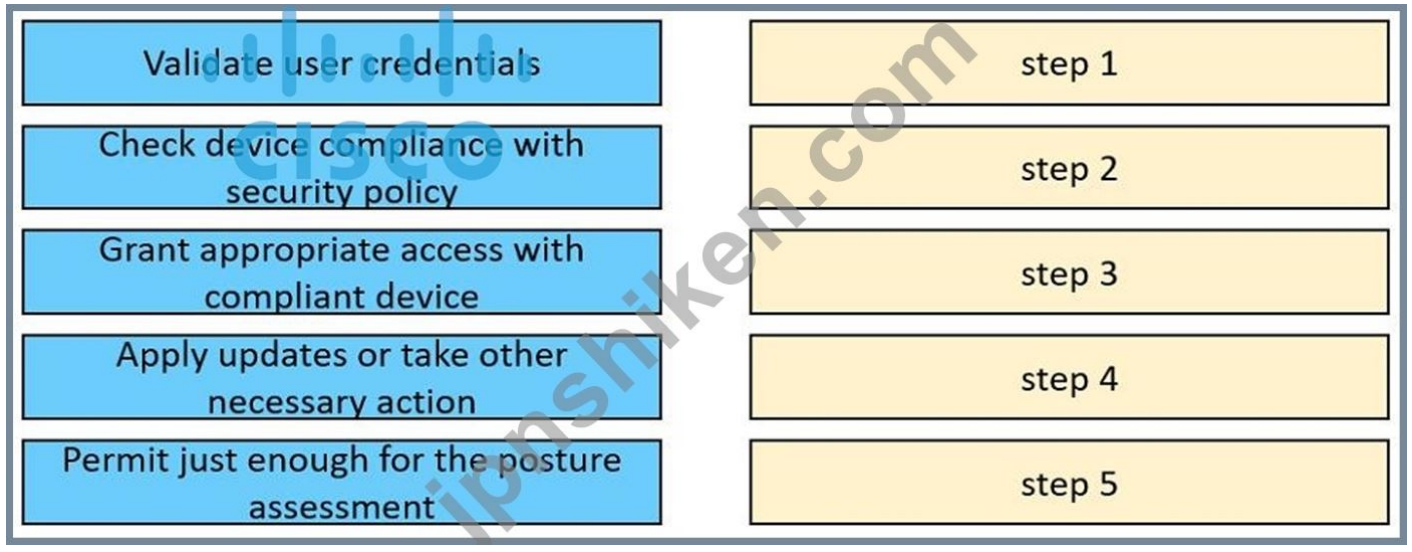
質問: **73**
攻撃者は、相互に通信している2つのホストの間に、どのタイプの攻撃でマシンを挿入しますか？
A. LDAPインジェクション
B. 中間者
C. クロスサイトスクリプティング
D. 安全でないAPI
正解: **(**正解を表示します**)**

質問: **74**
エンジニアはCiscoUmbrellaインテリジェントプロキシのSSL復号化を有効にしており、エンドユーザーに警告せずにトラフィックが検査されていることを確認する必要があります。
A. 組織のルートCAをUmbrella管理ポータルにアップロードします
B. UmbrellaルートCAをユーザーのデバイスの信頼されたルートストアにインポートします。
C. ユーザーのブラウザ設定を変更して、Umbrellaからのエラーを抑制します。
D. 信頼できるサードパーティの署名付き証明書を持つWebサイトのみへのアクセスを制限します。

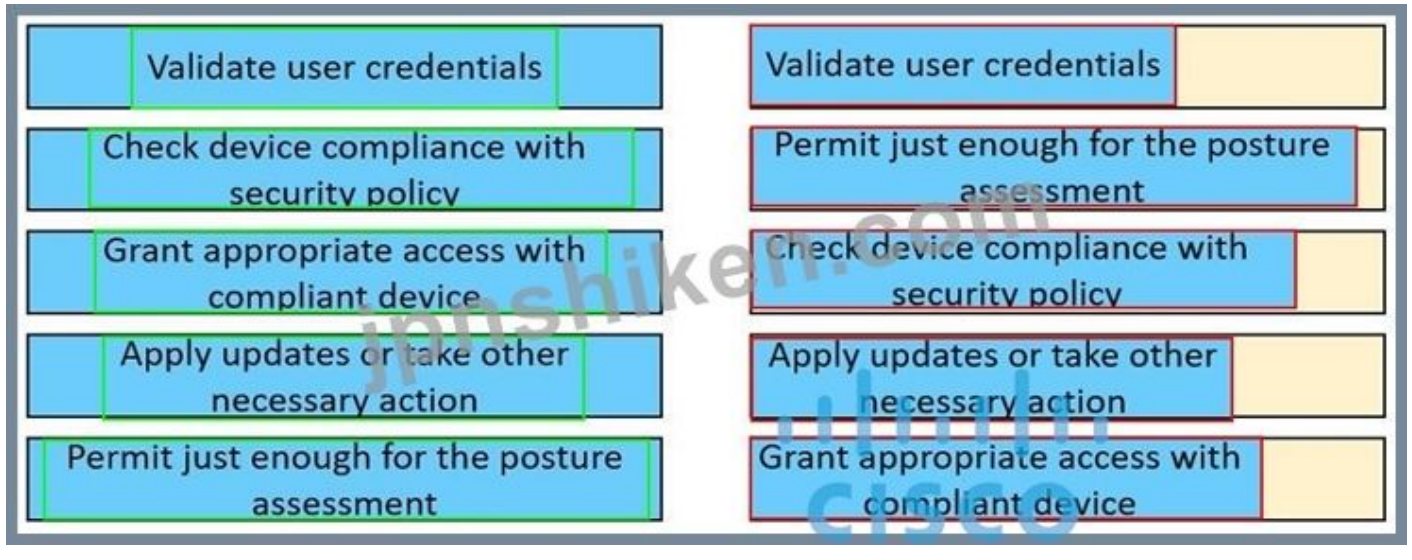
正解: (正解を表示します)

質問: **75**
脅威分析のためにプリロードされた動作インジケーター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. 高度なサンドボックス
B. 深い可視性スキャン
C. ポイントインタイムチェック
D. 高度なスキャン
正解: (正解を表示します)

質問: **76**
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。



正解:



質問: **77**
どのCiscoAMPファイルの処理が有効ですか？
A. マルウェア
B. 悪意のない
C. 汚れた
D. 手付かずの
正解: **A** (コメントを発表する)

質問: **78**
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. NetFlow
B. Flow
C. mirror port
D. VPC flow logs
正解: (正解を表示します)

質問: **79**
オンプレミスのCiscoWSAと比較してCiscoCWSを使用する利点は何ですか。
A. Cisco CWSは、Cisco WSAと比較して、内部ネットワークとセキュリティインフラストラクチャの負荷を最小限に抑えます。
B. Cisco CWSは、リモートワーカーのために本社を経由してトラフィックをバックホールする必要性を排除しますが、CiscoWSAはそうではありません。
C. SAASクラウドアプリケーションのコンテンツスキャンは、Cisco CWSからは利用できますが、CiscoWSAからは利用できません。
D. URLカテゴリは、CiscoWSAよりもCiscoCWSで頻繁に更新されます
正解: **B** (コメントを発表する)

質問: **80**
Cisco Tetrationを使用する利点は何ですか？
A. サーバーから施行データを収集し、パケット間変動を収集します。
B. ポリシーコンプライアンスデータとプロセスの詳細を収集します。
C. サーバーからテレメトリデータを収集し、ソフトウェアセンサーを使用してフロー情報を分析します。
D. サーバーからほぼリアルタイムのデータを収集し、サーバー上に存在するソフトウェアパッケージのインベントリを作成します。
正解: **A** (コメントを発表する)

質問: **81**
NetFlowバージョン9テンプレートレコードの目的は何ですか？
A. NetFlowプロセスのデータ形式を指定します。
B. 個々のデータレコードを区別するための一意の識別番号として機能します
C. IPフローに関する標準化された一連の情報を提供します。
D. Itはデータレコードの形式を定義します。
正解: **(**正解を表示します**)**

質問: **82**
IPsecのステートフルフェールオーバーの前提条件はどれですか。 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たIKE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。IPsec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、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なければなりません。
C. アクティブデバイスでセットアップされた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セットアップされた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**)**
Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not require adjustment or reconfiguration of any remote peer.
Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.
Prerequisites for Stateful Failover for IPsec
Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices This document assumes that you have a complete IKE and IPsec configuration.
The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device.
That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.
Reference:
Although the prerequisites only stated that "Both routers should be the same type of device" but in the
"Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active and standby devices must run the identical version of the Cisco IOS software" so answer E is better than answer B.

質問: **83**
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. 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
B. ゾーンに割り当てることができるインターフェイスは1つだけです
C. 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
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 (コメントを発表する)**

質問: **84**
管理者は、CiscoFMCでCiscoThreatIntelligenceDirectorを有効にします。どのプロセスがSTIXを使用し、ブロックリストのアップロードとダウンロードを許可しますか？
A. 消費
B. 共有
C. 編集
D. オーサリング
正解: **(正解を表示します)**

質問: **85**
Cisco DNA Center内で使用されるRESTfulアーキテクチャの2つの特徴は何ですか？ 2つ選択してください。）
A. RESTは、GET、PUT、POST、DELETEなどのメソッドを使用します。
B. RESTコードは任意のプログラミング言語でコンパイルできます。
C. RESTはHTTPを使用してWebサービスにリクエストを送信します。
D. RESTはLinuxプラットフォームベースのアーキテクチャです。
E. POSTアクションは、URLパスの既存のデータを置き換えます。
正解: **(正解を表示します)**

質問: **86**
ユーザーのパスワードが侵害された場合に、システムへの不正アクセスを阻止するソリューションはどれですか？
A. VPN
B. SSL
C. MFA
D. AMP
正解: **C (コメントを発表する)**

質問: **87**
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. Windowsレジストリ値
D. DHCPスヌーピングチェック

E. エンドポイント保護ソフトウェアバージョン
正解: **A,D** (コメントを発表する)

質問: **88**
サーバーレスアプリケーションについて説明しているステートメントはどれですか？
A. アプリケーションは、KubernetesまたはDockerSwarmによって管理されるコンテナ化された環境から実行されます。
B. サーバーファームの前にあるアプリケーション配信コントローラーは、アプリケーションが毎回実行されるサーバーを指定します。
C. アプリケーションは、物理サーバーではなくネットワーク機器にインストールされます。
D. アプリケーションは、クラウドプロバイダーによって完全に管理されている、一時的でイベントトリガーのステートレスコンテナーから実行されます。
正解: (正解を表示します)

質問: **89**
既知および未知の脅威に対するエンドポイントでの保護、検出、および応答を可能にするリモートワーカー向けのソリューションはどれですか？
A. Cisco Umbrella
B. Cisco AnyConnect
C. Cisco Duo
D. エンドポイント向けCisco AMP
正解: **D** (コメントを発表する)

質問: **90**
エンジニアは、DHCP セキュリティ メカニズムを実装しており、Cisco ISE 内で作成されたプロファイルに追加の属性を追加する機能を必要としています。このタスクを達成するアクションはどれですか?
A. DHCP オプション 82 を使用して、要求が正当なエンドポイントからのものであることを確認し、情報を Cisco ISE に送信します。
B. スイッチで MAC から IP アドレスへのマッピングを定義して、不正なデバイスが IP アドレスを取得できないようにします。
C. スイッチ VLAN で DHCP スヌーピングを構成し、必要なインターフェイスを信頼します。
D. DHCP リレーを変更し、IP アドレスを Cisco ISE にポイントします。
正解: **C** (コメントを発表する)

質問: **91**
展示を参照してください。

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

構成でこの認証プロトコルを使用すると、どのような結果になりますか?
A. 認証要求にはパスワードのみが含まれます。
B. 認証要求にはユーザー名のみが含まれます。
C. 認証と承認の要求は、1 つのパケットにグループ化されます。
D. 認証と認可のリクエスト パケットが別々にあります。

正解: **(**正解を表示します**)**

質問: **92**
RSAキーをエクスポートおよびインポートするときに、どのタイプの保護がRSAキーを暗号化しますか？
A. NGE
B. エクスポート不可
C. パスフレーズ
D. ファイル
正解: **(**正解を表示します**)**

質問: **93**
安全なアプリケーションを構築するために開発者が従わなければならない安全な開発慣行とガイドラインのコレクションから作成されたソリューションはどれですか？
A. OWASP
B. Fuzzing Framework
C. Radamsa
D. AFL
正解: **(**正解を表示します**)**

質問: **94**
アルゴリズムを選択する際、鍵の確立のために Diffie Hellman と RSA について何を考慮する必要がありますか?
A. RSA は、対称鍵を出力することを目的とした非対称鍵確立アルゴリズムです。
B. RSA は、非対称キーを出力するための対称キー確立アルゴリズムです。
C. DH は、非対称鍵を出力するための対称鍵確立アルゴリズムです。
D. DH は、対称鍵を出力するための非対称鍵確立アルゴリズムです。
正解: **D (**コメントを発表する**)**
Diffie Hellman (DH) uses a private-public key pair to establish a shared secret, typically a symmetric key. DH is not a symmetric algorithm - it is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm.

質問: **95**
管理者は、ネットワーク管理システムがSNMPv3を使用してホストをアクティブに監視できるように、ASDMを介してCiscoASAを設定する必要があります。この構成で実行する必要がある2つのタスクはどれですか？
（2つ選択してください。）

A. SNMPマネージャーとUDPポートを指定します。
B. SNMPUSMエントリを追加します
C. SNMPユーザーグループを指定します
D. コミュニティ文字列を指定します。
E. SNMPホストアクセスエントリを追加します
正解: **(**正解を表示します**)**

質問: **96**
Cisco AMP for Endpointsはどのように次世代の保護を提供しますか？
A. CiscoFTDデバイスと統合します。
B. ランサムウェアから保護するために、ユーザーエンドポイント上のデータを暗号化します。
C. エンドポイント保護プラットフォームとエンドポイントの検出と応答を活用します。
D. Cisco pxGridを利用して、CiscoAMPが脅威インテリジェンスセンターから脅威フィードをプルできるようにします。
正解: **(**正解を表示します**)**

質問: **97**
AWSのCiscoFTDvでサポートされている2つの導入モデル構成はどれですか。 （2つ選択してください。）
A. 1つの管理インターフェイスと2つのトラフィックインターフェイスが設定されたCisco FTDv
B. ルーテッドモードで設定され、オンプレミスの物理FMCアプライアンスによって管理されるCiscoFTDv
C. ルーテッドモードで設定されたCiscoFTDvおよび設定されたIPv6
D. ルーテッドモードで設定され、AWSにインストールされたFMCvによって管理されるCisco FTDv
E. 2つの管理インターフェイスと1つのトラフィックインターフェイスが設定されたCisco FTDv
正解: **(**正解を表示します**)**

質問: **98**
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: **(**正解を表示します**)**
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.
TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.
TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.
Although there is no "binding" capability in the list but it is the best answer here.

質問: **99**

2つのトロイの木馬マルウェア攻撃とは何ですか？　2つ選択してください）
A. ルートキット
B. スマーフ
C. バックドア
D. 同期
E. フロントドア
正解: **(**正解を表示します**)**

質問: **100**
Cisco Stealthwatchシステムは、ルータ、スイッチ、およびファイアウォールからどのタイプのデータを収集して分析しますか。
A. SNMP
B. syslog
C. NTP
D. NetFlow
正解: **(**正解を表示します**)**

質問: **101**
Cisco WSAログファイルに保存されるURIテキストの量を制御するアクションはどれですか。
A. 最大パケットサイズを設定します。
B. datasecurityconfigコマンドを設定します
C. 小さいログエントリサイズを設定します。
D. HTTPSサブコマンドを使用してadvancedproxyconfigコマンドを構成します
正解: **(**正解を表示します**)**

質問: **102**
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. スマーフ
B. MITM
C. ティアドロップ
D. 土地
正解: **(**正解を表示します**)**
A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

質問: **103**
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、メッセージのコピーを配信し、メッセージを追加してDLP違反としてフラグを立て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. コピーを他の受信者に配信および送信する
B. DLP違反通知を隔離して送信する
C. DLP違反でサブジェクトヘッダーを隔離および変更する
D. 免責事項のテキストを配信して追加する
正解**: (**正解を表示します**)**
You specify primary and secondary actions that the appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities.
Primary actions include:
- Deliver
- Drop
- Quarantine
Secondary actions include:
- Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.
- Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers.
- Altering the subject header of messages containing a DLP violation.
- Adding disclaimer text to messages.
- Sending messages to an alternate destination mailhost.
- Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)
- Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer.
Reference:
b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

質問**: 104**
ユーザーがセキュリティの脅威を見つけるように訓練されており、ネットワークデバイスがすでに脅威の防止に役立っているにもかかわらず、エンドポイントに論理的なセキュリティ制御を設定することが重要なのはなぜですか？
A. エンドポイントをより多くの脅威にさらす
B. エンドポイントの盗難を防ぐため
C. ヒューマンエラーまたは内部脅威が依然として存在するため
D. 多層防御がネットワークで停止するため
正解**: C (**コメントを発表する**)**

質問**: 105**
Cisco FTDvはASAvを介してどのような機能を提供しますか？
A. Cisco FTDvは1GBのファイアウォールスループットを提供しますが、CiscoASAvは提供しません
B. Cisco FTDvはURLフィルタリングをサポートしていますが、ASAvはサポートしていません
C. Cisco FTDvはAWSで実行されますが、ASAvは実行されません

D. Cisco FTDvはVMWareで実行されますが、ASAvは実行されません
正解: **B** (コメントを発表する)

質問: **106**
エンジニアがDropboxとCiscoCloudlockの統合を構成しています。Dropbox管理コンソールでAPIアクセスを許可する前に、どのアクションを実行する必要がありますか？
A. CiscoCloudlockポータルのCiscoCloudlock認証およびAPIセクションにDropboxを追加します。
B. Dropbox管理ポータルからCiscoCloudlockにAPIリクエストを送信します。
C. CiscoCloudlockポータルのプラットフォーム設定内でDropboxを承認します。
D. Dropbox管理ポータルにCiscoCloudlockを追加します。
正解: **C** (コメントを発表する)

質問: **107**
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、認証に使用するユーザー名とパスワードを取得します。
B. 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
C. 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。
D. 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。
正解: (正解を表示します)

質問: **108**
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)
Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-faq-cte-en.html
Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-faq-cte-en.html

質問: **109**

プライベートクラウドインスタンスと比較して、Cisco AMPパブリッククラウドインスタンス専用の機能はどれですか？
A. RBAC
B. SPERO検出エンジン
C. ETHOS検出エンジン
D. TETRA検出エンジン
正解: **(**正解を表示します**)**

質問: **110**
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**)**
CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port 1700, while the actual RFC calls out using UDP port 3799.

質問: **111**
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. CNAME
B. MX
C. DKIM
D. SPF
正解: **B (**コメントを発表する**)**

質問: **112**
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. 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 provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software).

質問: **113**

IPsecで使用される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 (**コメントを発表する**)**
Cryptographic algorithms defined for use with IPsec include:
+ HMAC-SHA1/SHA2 for integrity protection and authenticity.
+ TripleDES-CBC for confidentiality
+ AES-CBC and AES-CTR for confidentiality.
+ AES-GCM and ChaCha20-Poly1305 providing confidentiality and authentication together efficiently.

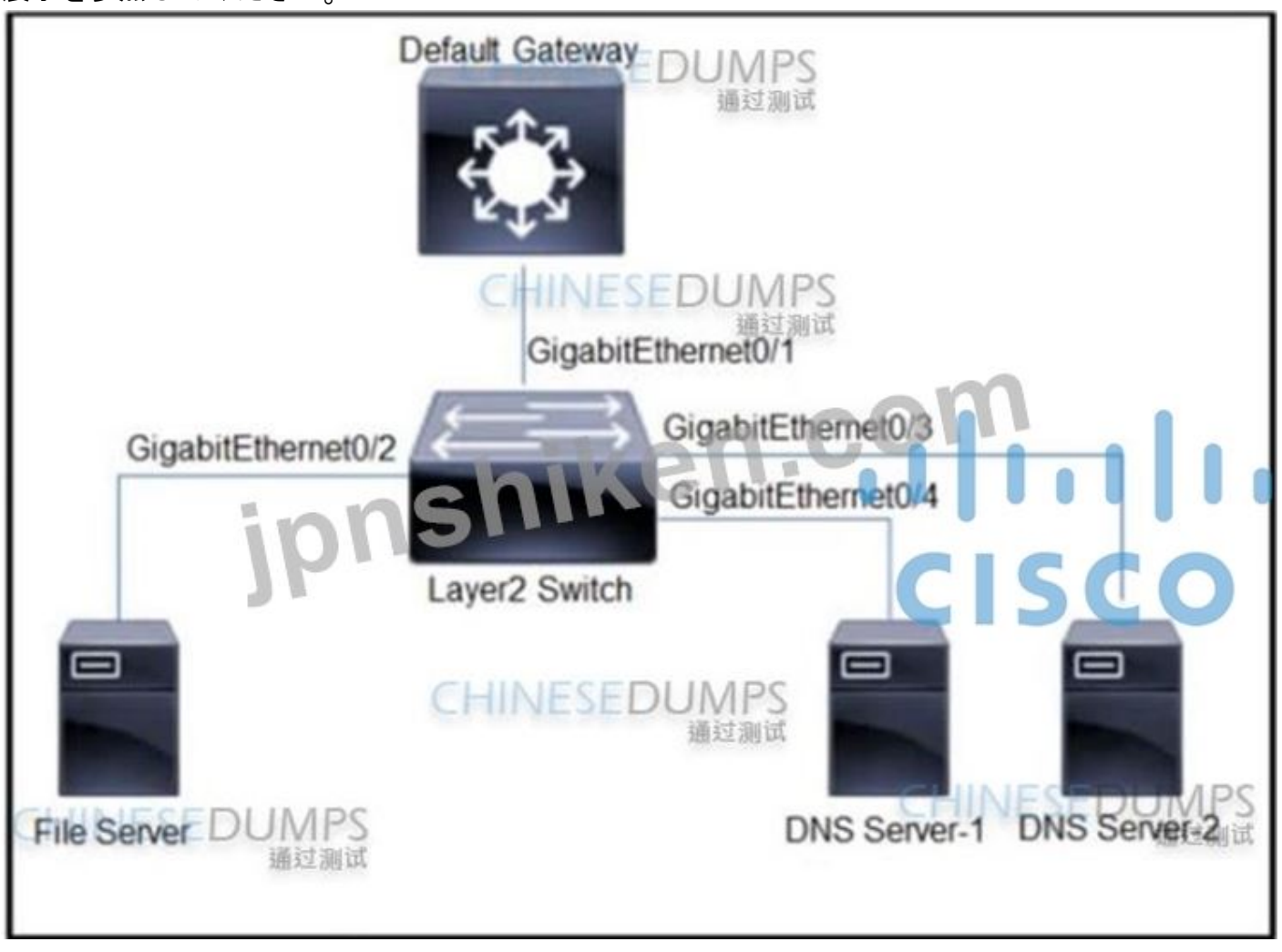
質問: **114**
エンドポイントにインストールされた場合のCiscoUmbrella Roamingの役割は何ですか？
A. 悪意のあるファイル転送からエンドポイントを保護するため
B. 企業ネットワークの内外の悪意のあるリンクから資産を保護するため
C. 企業ネットワークへの安全なVPN接続を確立するため
D. 姿勢コンプライアンスと必須ソフトウェアを実施する
正解: **(**正解を表示します**)**
Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN.

質問: **115**
Cisco Advanced Phishing Protection ソリューションがユーザを保護する 2 つの方法はどれですか? （2つ選んでください。）
A. センサーを使用してトロイの木馬マルウェアを防止します。
B. ユーザーの受信トレイから悪意のあるメールを自動的に削除します。
C. ビデオ会議で共有されるすべてのパスワードを保護します。
D. インターネットからのゼロデイ攻撃をすべて防ぎます。
E. 侵害されたアカウントの使用とソーシャル エンジニアリングを防止します。
正解: **(**正解を表示します**)**

質問: **116**
インターネットブラウザを使用してクラウドベースのサービスにアクセスすると、どのようなリスクが発生しますか？
A. クラウドコネクタへの断続的な接続
B. プロトコル内の脆弱性
C. 不正アクセスを許可するインフラストラクチャの構成ミス
D. APIの安全でない実装
正解: **(**正解を表示します**)**

質問: **117**
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. コマンドと制御
D. 許可されたアプリケーション
E. URL
正解: **(**正解を表示します**)**
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.
A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

質問: **118**
展示を参照してください。



展示を参照してください。すべてのサーバーは同じ VLAN/サブネットにあります。DNS サーバー 1 と DNS サーバー 2 は相互に通信する必要があり、すべてのサーバーはデフォルト ゲートウェイ マルチレイヤ スイッチと通信する必要があります。DNS サーバーとファイル サーバー間の通信を防止するには、どの種類のプライベート VLAN ポートを構成する必要がありますか?
A. GigabitEthernet0/1 をコミュニティ ポートとして、GigabitEthernet0/2 を隔離ポートとして、GigabitEthernet0/3 と GigabitEthernet0/4 を無差別ポートとして構成します。
B. GigabitEthernet0/1 をプロミスキャス ポートとして、GigabitEthernet0/2 を独立ポートとして、GigabitEthernet0/3 および GrgabitEthernet0/4 をコミュニティ ポートとして構成します。
C. GigabitEthernet0/1 をコミュニティ ポートとして、GigabitEthernet0/2 をプロミスキャス ポートとして、Gigabit Ethernet0/3 および GigabitEthernet0/4 を独立ポートとして構成します。
D. GigabitEthernet0/1 をプロミスキャス ポートとして、GigabitEthernet0/2 をコミュニティ ポートとして、GigabitEthernet0/3 と GrgabitEthernet0/4 を独立ポートとして構成します。
正解: **B** (コメントを発表する)

質問: **119**
WCCPで設定されたルータは、Cisco WSAが機能しているかどうかをどのように識別しますか？
A. WSAは10秒ごとにHere-I-Amメッセージを送信し、ルータはISee-Youメッセージで確認応答します。
B. ルータとWSAの間でICMP pingが3回連続して失敗した場合、トラフィックはWSAに送信されなくなります。
C. ルータとWSAの間でICMP pingが3回連続して失敗した場合、トラフィックはルータに送信されなくなります。
D. ルータは10秒ごとにHere-I-Amメッセージを送信し、WSAはISee-Youメッセージで確認応答します。
正解: (正解を表示します)

質問: **120**
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)
The syntax of this command is shown below:
snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list] The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

質問: **121**
認証局によって実行される機能はどれですか？ただし、登録局の制限はありますか？
A. ユーザーIDの確認
B. 登録リクエストを受け付けます
C. 証明書の再登録
D. CRLパブリッシング
正解: **(**正解を表示します**)**

質問: **122**
顧客がクラウドサービスプロバイダーによってホスト、管理、および保守されているWebアプリケーションにアクセスできるようにするクラウドサービスオファリングはどれですか？
A. IaC
B. PaaS
C. IaaS
D. SaaS
正解: **(**正解を表示します**)**

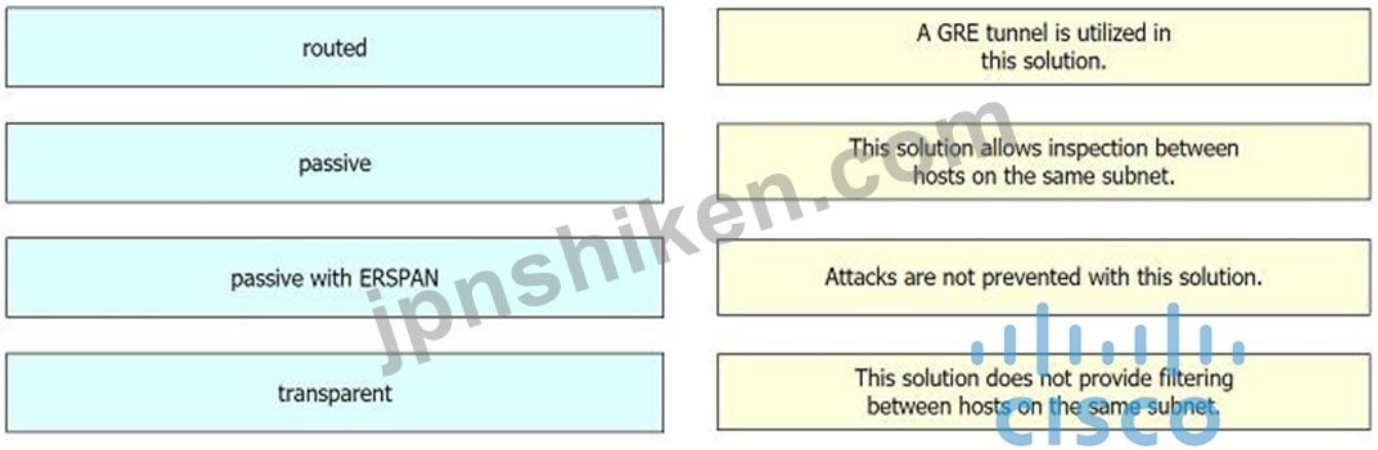
質問: **123**
NetFlowを使用して、ネットワーク、データセンター、ブランチオフィス、およびクラウド全体の可視性を提供するセキュリティソリューションはどれですか。
A. Cisco Umbrella
B. Cisco Encrypted Traffic Analytics
C. Cisco Stealthwatch
D. Cisco CTA
正解: **(**正解を表示します**)**

質問: **124**
VPN展開内でFlexVPNを介してGETVPNを使用する利点は何ですか？
A. GETVPNはリモートアクセスVPNをサポートします
B. GETVPNはシスコ以外のデバイスと相互運用します
C. GET VPNは、接続に複数のセキュリティアソシエーションを使用します
D. GET VPNは、MPLSおよびプライベートIPネットワークをネイティブにサポートします

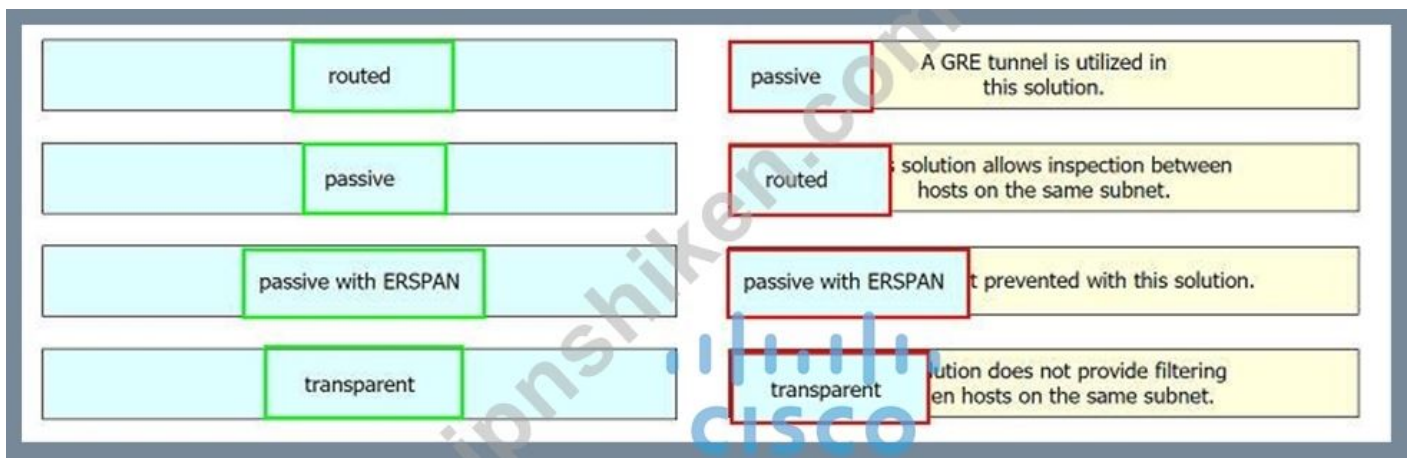
正解: **(**正解を表示します**)**

質問: **125**
つのDDoS攻撃のカテゴリは何ですか？　2つ選択してください）
A. sequential
B. protocol
C. database
D. volume-based
E. screen-based
正解: **(**正解を表示します**)**
There are three basic categories of attack:
+ volume-based attacks, which use high traffic to inundate the network bandwidth
+ protocol attacks, which focus on exploiting server resources
+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks Reference:
https://www.esecurityplanet.com/networks/types-of-ddos-attacks/

質問: **126**
左側の配置モデルを右側の説明にドラッグ アンド ドロップします。



正解:



質問: **127**

エンジニアは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-256
B. ESP
C. AES-192
D. IKEv1
正解: **(**正解を表示します**)**

質問: **128**
ハッカーが悪意のあるコードをWebアプリケーションを介して無防備なユーザーに送信し、被害者のWebブラウザにコードの実行を要求するために使用する攻撃方法はどれですか。
A. SQLインジェクション
B. クロスサイトスクリプティング
C. バッファオーバーフロー
D. ブラウザWGET
正解: **(**正解を表示します**)**

質問: **129**
組織が認証のためにMFA戦略に移行する必要があるのはなぜですか？
A. MFAは、認証メカニズムの証拠を必要としません。
B. 生体認証は、ハッキングされやすいため、MFAが必要になります。
C. MFA認証方法が危険にさらされることはありません。
D. 単一の認証方法は、MFAよりも簡単に侵害される可能性があります。
正解: **(**正解を表示します**)**

質問: **130**
NIST 800-145ガイドに基づいて、コミュニティ内の1つ以上の組織、サードパーティ、またはそれらの組み合わせによって所有、管理、運用されるクラウドアーキテクチャはどれですか？また、オンプレミスまたはオフプレミスに存在する可能性がありますか？
A. コミュニティクラウド
B. ハイブリッドクラウド
C. パブリッククラウド
D. プライベートクラウド
正解: **A (**コメントを発表する**)**

質問: **131**
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Cisco StealthwatchCloud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、この要件を満たすには何をする必要がありますか？
A. syslogをCisco StealthwatchCloudに送信するようにCiscoFMCを設定します
B. Cisco StealthwatchCloudにデータを送信するCiscoStealthwatch CloudPNM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Cisco StealthwatchCloudに送信します
D. NetFlowをCisco StealthwatchCloudに送信するようにCiscoFMCを設定します
正解: **B** (コメントを発表する)
The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. - VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

質問: **132**
エンジニアがCiscoWSAを設定しており、インターネットおよびLANからの個別の電子メール転送フローを有効にする必要があります。この目標を達成するには、どの展開モードを使用する必要がありますか？
A. 単一のインターフェース
B. 透明
C. マルチコンテキスト
D. 2つのインターフェース
正解: **D** (コメントを発表する)

質問: **133**
CiscoIOSルータでIKEv1Phase1用にISAKMPを設定する場合、管理者はコマンドcrypto isakmp key cisco address0.0.0.0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)
The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of "0.0.0.0" will authenticate any address with this key

質問: **134**
ある企業が最近、abc428565580xyz exe という名前のファイルを介して Windows ネットワーク全体に広がる攻撃を発見しました。悪意のあるファイルは AMP for Endpoints ポータルのシンプル カスタム検出リストにアップロードされ、Windows クライアントに現在適用されているポリシーは検出リストを参照するように更新されました。既知の感染システムでの検証テスト スキャンは、AMP for Endpoints がこのファイルの存在を侵害の指標として検出していないことを示しています。悪意のあるファイルを確実に検出するには、何を実行する必要がありますか?
A. ファイルの SHA-256 ハッシュをシンプル カスタム検出リストにアップロードします。
B. 悪意のあるファイルをブロックされたアプリケーション コントロール リストにアップロードします。
C. シンプルなカスタム検出リストの代わりに高度なカスタム検出リストを使用する
D. 動的分析のためにファイルを Cisco Threat Grid に送信するには、ポリシー設定のボックスをオンにします。
正解: (正解を表示します)

質問: **135**
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。
B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **136**
Cisco ISE内のどの機能が、ネットワークへのアクセスを提供する前にエンドポイントのコンプライアンスを検証しますか。
A. pxGrid
B. プロファイリング
C. 姿勢
D. MAB
正解: **C (**コメントを発表する**)**

質問: **137**
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、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。
B. Cisco ASA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。
C. 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。
D. 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
正解: **A (**コメントを発表する**)**

質問: **138**
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. dot1x system-auth-control
B. aaa new-model
C. dot1xpaeオーセンティケーター
D. 認証ポート制御自動
正解: **(**正解を表示します**)**

質問: **139**
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、分析が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: **C (**コメントを発表する**)**
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.
Reference:
In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.

質問: **140**
Cisco Next Generation Firewall Virtualをサポートしているパブリッククラウドプロバイダーはどれですか？
A. Google Cloud Platform
B. Red HatEnterpriseの視覚化
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 NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.

In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

質問**: 141**
エンドポイントがネットワークに接続することを許可する前に、どのCiscoISEサービスがエンドポイントのコンプライアンスをチェックしますか。
A. posture
B. profiler
C. Threat Centric NAC
D. Cisco TrustSec
正解**: A (**コメントを発表する**)**

質問**: 142**
ネットワークやシステムを危険にさらす可能性のある有害なイベントを軽減するのに役立つ、脅威と脅威アクターに関する情報を持つための用語は何ですか？
A. 信頼できる自動交換
B. 脅威インテリジェンス
C. エクスプロイトデータベース
D. 侵入の痕跡
正解**: B (**コメントを発表する**)**

質問**: 143**
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 (**コメントを発表する**)**
Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.

質問**: 144**
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: **145**
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. EPG内分離
D. 別々のEPGに配置
正解: **(**正解を表示します**)**
Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another.

質問: **146**
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. インテリジェントプロキシを有効にします。
B. SSL復号化をアクティブにします。
C. Advanced Malware Protectionライセンスをアクティブ化
D. IPレイヤーの適用を有効にします。
正解: **A (**コメントを発表する**)**

質問: **147**
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ながら、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WCCPを使用して透過的なトラフィックリダイレクションを設定します
B. 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ションを設定します
C. 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。
D. 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
正解: **(**正解を表示します**)**

質問: **148**
Cisco AMPがWebセキュリティに追加されると、どの機能が含まれますか。
A. 多要素認証ベースのユーザーID
B. 電子メールでのフィッシング検出
C. 不明なファイルの動作の詳細な分析

D. 感染したエンドポイントでの脅威の防止
正解: **(**正解を表示します**)**

質問: **149**
顧客は、イントラネットを含むさまざまな外部HTTPリソースを利用できます。エクストラネット、およびプロキシ構成が明示モードで実行されているインターネットクライアントデスクトップブラウザーを構成して、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できるようにする方法はどれですか。
A. ブリッジモード
B. 透過モード
C. PACファイル
D. ファイルを転送
正解: **(**正解を表示します**)**

質問: **150**
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. 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。
B. 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。
C. 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。
D. 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
正解: **(**正解を表示します**)**
The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

質問: **151**
アプリケーションの可視性とセグメンテーションでハイブリッドクラウド展開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. ネクサス
C. ステルスウォッチ
D. テトレーション
正解: **(**正解を表示します**)**

質問: **152**
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. 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。
D. 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。
E. 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。
正解: **(**正解を表示します**)**

質問: **153**
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. DNSルックアップのレジストリを変更する
B. ActiveDirectoryグループポリシーを使用してCiscoUmbrellaDNSサーバーを適用する
C. 企業のネームサーバーにDNSクエリを強制する
D. CiscoUmbrellaローミングクライアントを使用する
正解: **(**正解を表示します**)**

質問: **154**
組織は、クラウドで提供されるSaaSベースのソリューションを実装して、AWSネットワーク全体で可視性と脅威の検出を提供したいと考えています。ソリューションはソフトウェアエージェントなしでデプロイする必要があり、代わりにAWSVPCフローログに依存する必要があります。これらの要件を満たすソリューションはどれですか？
A. Cisco Stealthwatch Cloud
B. NetFlow collectors
C. Cisco Umbrella
D. Cisco Cloudlock
正解: **(**正解を表示します**)**

質問: **155**
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. FlexVPNは複数のSAを使用し、DMVPNは使用しないため
D. DMVPNは複数のSAを使用し、FlexVPNは使用しないため
正解: **C (**コメントを発表する**)**
FlexVPN supports IKEv2 -> Answer A is not correct.
DMVPN supports both IKEv1 & IKEv2 -> Answer B is not correct.
FlexVPN support multiple SAs -> Answer D is not correct.

質問: **156**
PKIにおける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**)**
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.

質問: **157**
NetFlowセキュアイベントロギングの機能は何ですか？
A. 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。
B. v5およびv8テンプレートをサポートします。
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. 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。
正解: **(**正解を表示します**)**

質問: **158**
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アドレスを構成します
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* .domain.comアドレスを構成します
D. ブロックリストで* .comアドレスを設定します。
正解: **B (**コメントを発表する**)**

質問: **159**
展示を参照してください。

このデバイスがポートに接続しようとするとどうなりますか？

A. 802.1Xは機能せず、デバイスはネットワークアクセスを許可されません

B. 802 1Xが機能し、デバイスはネットワーク上で許可されます

C. 802 1XとMABの両方が使用され、ISEはポリシーを使用してアクセスレベルを決定できます

D. 802.1Xは機能しませんが、MABが起動し、ネットワーク上のデバイスを許可します。

正解: **(**正解を表示します**)**

質問: **160**

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. 受信コンテンツフィルターを構成する

B. バウンス検証を使用する

C. ディレクトリハーベスト攻撃防止を構成する

D. 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

正解: **C (**コメントを発表する**)**

A Directory Harvest Attack (DHA) is a technique used by spammers to find valid/existent email addresses at a domain either by using Brute force or by guessing valid e-mail addresses at a domain using different permutations of common username. Its easy for attackers to get hold of a valid email address if your organization uses standard format for official e-mail alias (for example: jsmith@example.com). We can configure DHA Prevention to prevent malicious actors from quickly identifying valid recipients.

Note: Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server, such as ClickMail Central Directory. For example, here's an LDAP search translated into plain English: "Search for all people located in Chicago who's name contains "Fred" that have an email address. Please return their full name, email, title, and description.

質問: **161**

ルーターに NetFlow を実装する前に、どの機能を構成する必要がありますか?

A. VRF

B. SNMPv3

C. IP ルーティング
D. シスログ
正解: **(**正解を表示します**)**

質問: **162**
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. 管理者が悪意のあるファイルを隔離して、悪意を持ってではなく、アプリケーションが機能できるようにします。
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. アプリケーション情報を管理者に送信して対処します。
正解: **(**正解を表示します**)**

質問: **163**
Cisco DuoをMFAソリューションとして使用する2つの利点は何ですか？ 2つ選択してください。）
A. 複数のクラウドプラットフォームまたはオンプレミス環境間でアプリケーションを保護するのに役立つネイティブ統合
B. エンドポイントに保存されているデータを暗号化します
C. 複数のアプリケーションとユーザーにシンプルで合理化されたログインエクスペリエンスを提供します
D. 紛失または盗難にあったデバイスをリモートでワイプする方法を管理者に付与します
E. エンドポイントデバイスのアプリケーションと構成を一元管理できます
正解: **(**正解を表示します**)**

質問: **164**
ASAブリッジグループの展開では、ブリッジグループごとにいくつのインターフェイスがサポートされていますか。
A. 最大2
B. 最大4
C. 最大8
D. 最大16
正解: **(**正解を表示します**)**
Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.
As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.
Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

質問: **165**
ネットワークの可視性、脅威の検出、分析をパブリッククラウド環境に拡張するシスコのソリューションはどれですか。
A. Cisco Appdynamics
B. Cisco Umbrella
C. Cisco CloudLock
D. Cisco Stealthwatch Cloud

正解: (正解を表示します)

質問: **166**
Cisco ISEとpxGridを相互に、および他の相互運用可能なセキュリティプラットフォームと統合するために使用される業界標準はどれですか。
A. ANSI
B. IETF
C. NIST
D. IEEE
正解: (正解を表示します)

質問: **167**
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 1 md5Cisc392368270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構成しています。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: **B** (コメントを発表する)
To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands:
NTP_Server(config)#ntp authentication-key 2 md5 securitytut
NTP_Server(config)#ntp authenticate
NTP_Server(config)#ntp trusted-key 2
Then you must configure the same authentication-key on the client router:
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
Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example:
Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

質問: **168**

プライベートネットワーク、パブリッククラウド、暗号化されたトラフィック全体の脅威を検出するソリューションはどれですか？
A. Cisco Encrypted Traffic Analytics
B. Cisco Umbrella
C. Cisco Stealthwatch
D. Cisco CTA
正解: **(**正解を表示します**)**

質問: **169**
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、フィッシングなどの脅威をホストしているときにドメインが確実にブロックされるようにする機能は何ですか。
A. ファイル分析
B. コンテンツカテゴリのブロック
C. セキュリティカテゴリのブロック
D. アプリケーション制御
正解: **(**正解を表示します**)**

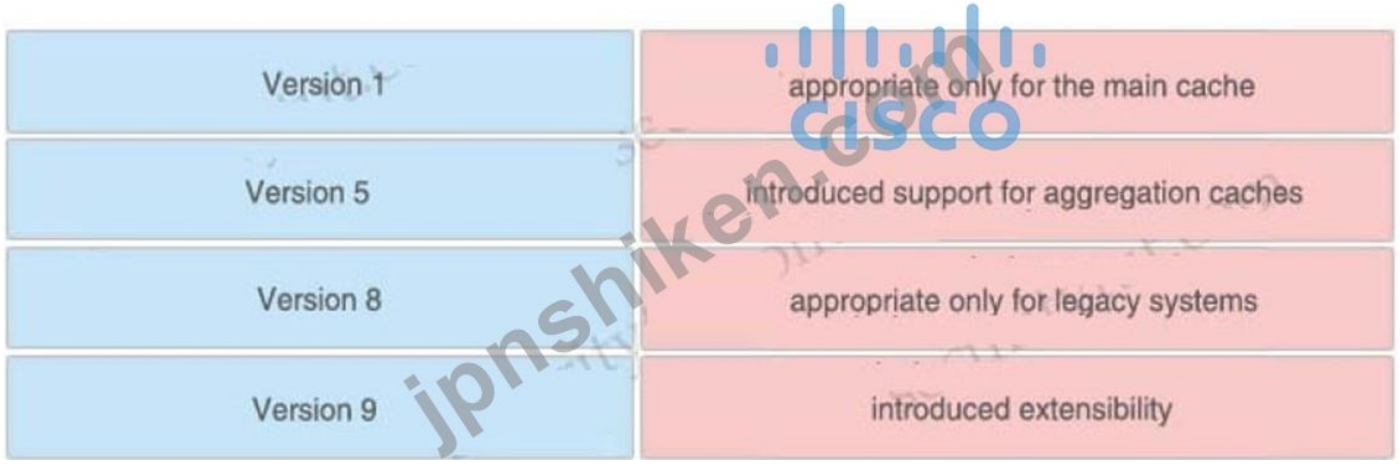
質問: **170**
BYODソリューションのエンドポイントのポスチャ評価に使用されるセキュリティソリューションはどれですか？
A. Cisco FTD
B. Cisco ASA
C. Cisco ISE
D. Cisco Umbrella
正解: **(**正解を表示します**)**

質問: **171**
欺瞞的なフィッシングとスピア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、経営幹部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. スピア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. スピアフィッシングとは、攻撃が組織の経営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 (**コメントを発表する**)**
In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.
Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information - and craft a fake email tailored for that person.

質問: **172**
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形式とは何ですか？
A. STIX
B. XMPP

C. pxGrid
D. SMTP
正解: **(**正解を表示します**)**
TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

質問: **173**
NetFlowエクスポート形式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: **174**
ネットワーク管理者がCiscoWSAでActiveDirectoryを使用してユーザーを透過的に識別する2つの方法は何ですか。2つ選択してください。)
A. NTLMまたはKerberos認証レルムを作成し、透過的なユーザー識別を有効にします。
B. LDAP認証レルムを作成し、透過的なユーザー識別を無効にします。
C. 別のeDirectoryサーバーを導入します。へこみIPアドレスはこのサーバーに記録されます。
D. eDirectoryクライアントを各クライアントワークステーションにインストールする必要があります。
E. Cisco ContextDirectoryAgentなどの別のActiveDirectoryエージェントを展開します。
正解: **(**正解を表示します**)**

質問: **175**
ネットワークエンジニアがsnmp-serveruserasmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxxコマンドを入力し、SNMP情報を10.255.255.1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. 10.255.255.1snmpv3asmith内のsnmp-serverホスト
B. 10.255.255.1snmpv3myv7内のsnmp-serverホスト
C. 10.255.255.1バージョン3myv7内のsnmp-serverホスト
D. 10.255.255.1バージョン3asmith内のsnmp-serverホスト
正解: **(**正解を表示します**)**

質問: **176**
Cisco AMP for Networksを使用する場合、分析のためにファイルをCisco AMP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: **(**正解を表示します**)**
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Reference:
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid.
Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.
There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.

質問: **177**
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: **(**正解を表示します**)**
In its essence, FlexVPN is the same as DMVPN. Connections between devices are still point-to-point GRE tunnels, spoke-to-spoke connectivity is still achieved with NHRP redirect message, IOS routers even run the same NHRP code for both DMVPN and FlexVPN, which also means that both are Cisco's proprietary technologies.

質問: **178**
サイバー脅威情報の交換を自動化するために使用される標準はどれですか?
A. MITRE
B. IoC
C. TAXII
D. STIX
正解: **(**正解を表示します**)**

質問: **179**
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. 明示的なプロキシ展開として定義されています。
B. 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。
C. ブリッジプロキシ展開として定義されます。
D. 透過プロキシ展開として定義されています。
E. 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。
正解: **(**正解を表示します**)**

質問: **180**
ポリシーの変更後にセッションを強制的に調整するには、Cisco ISE および Cisco TrustSec デバイスで行う必要がある 2 つの設定はどれですか? (2つ選んでください)
A. AAA サーバーの半径の動的作成者
B. 姿勢評価
C. aaa 承認 exec デフォルト ローカル
D. tacacs-server ホスト 10.1.1.250 キー パスワード
E. CoA
正解: **(**正解を表示します**)**

質問: **181**
MDMは、デバイス管理に関して組織に2つの利点を提供しますか？ 2つ選択してください。）
A. 許可されたアプリケーション管理
B. 資産在庫管理
C. 重要なデバイス管理
D. ネットワークデバイス管理
E. Active Directoryグループポリシー管理
正解: **(**正解を表示します**)**

質問: **182**
企業に次世代のエンドポイントセキュリティソリューションが選択された場合、実装を正当化するのに役立つ2つの主要な成果物は何ですか？ 2つ選択してください。）
A. グローバル脅威インテリジェンスセンターからのリアルタイムフィード
B. 接続されたエンドポイントを安全に保つためのマクロベースの保護
C. 接続されたエンドポイントにあるすべてのファイルの継続的な監視
D. 会社のエンドポイントでの署名ベースのエンドポイント保護
E. 電子メールにある悪意のあるコンテンツからエンドポイントを保護するための電子メール統合
正解: **(**正解を表示します**)**

質問: **183**
エンジニアは、データ転送の可視性とデータ流出に対する保護のために、Cisco Umbrella、Cisco CloudLock、Cisco Stealthwatch、またはCisco AppDynamics Cloud Monitoring のいずれを使用するかを決定しようとしています。これらの要件に最適なソリューションはどれですか?
A. Cisco CloudLock
B. Cisco Umbrella
C. Cisco Stealthwatch
D. Cisco AppDynamics Cloud Monitoring
正解: **(**正解を表示します**)**

質問: **184**
DMVPNはGETVPNよりもどのようなメリットがありますか？
A. DMVPNは非IPプロトコルをサポートし、GETVPNはIPプロトコルのみをサポートします。
B. DMVPNはパブリックインターネット経由で使用でき、GETVPNにはプライベートネットワークが必要です。
C. DMVPNはQoS、マルチキャスト、およびルーティングをサポートし、GETVPNはQoSのみをサポートします。
D. DMVPNはトンネルレスVPNであり、GETVPNはトンネルベースです。
正解: **(**正解を表示します**)**

質問: **185**
Cisco Identity Services Engineを使用して接続されたエンドポイントの属性を収集するように設定されている2つのプローブはどれですか？
2つ選択してください。）
A. TACACS +
B. DHCP

C. RADIUS
D. SMTP
E. sFlow
正解: **B,C (**コメントを発表する**)**

質問: **186**
プロファイリングで使用されるエンドポイント属性を収集するために、Cisco ISE は何を使用しますか?
A. 姿勢評価
B. Cisco AnyConnect セキュア モビリティ クライアント
C. Cisco pxGrid
D. プローブ
正解: **(**正解を表示します**)**

質問: **187**
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. W32/AutoRunワーム
B. スペクターワーム
C. 永遠の青い窓
D. ハートブリードSSLバグ
正解: **(**正解を表示します**)**

質問: **188**

エンジニアは、デバイス管理のためのTACACS +認証および承認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802.1X、MAB、またはWebAuthの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。
これらの要件をすべて満たす製品はどれですか？
A. Cisco Prime Infrastructure
B. Cisco Identity Services Engine
C. エンドポイント向けCisco AMP
D. Cisco Stealthwatch
正解: **B** (コメントを発表する)

質問: **189**
管理者はASDMを介してCiscoASAでNIPを設定しており、不正なNTPサーバが信頼できるタイムソースとして自分自身を挿入できないようにする必要があります。このタスクを実行するには、どの2つの手順を実行する必要がありますか。 2つ選択してください）
A. NTP階層を構成します
B. NTPサーバーと同期するためのインターフェースを選択します
C. 認証キーを設定します
D. NTPバージョンを指定します
E. NTPDNSホスト名を設定します
正解: (正解を表示します)

質問: **190**
ある会社が、ファイルを介してネットワークを介して伝播する攻撃を発見しました。将来これを追跡し、他のエンドポイントが感染したファイルを実行しないようにするために、カスタムファイルポリシーが作成されました。さらに、テスト中に、スキャンが侵入の痕跡としてファイルを検出していないことが発見されました。作成されたものが正常に機能していることを確認するには、何をする必要がありますか？
A. ファイルのダウンロード元のWebサイトのIPブロックリストを作成します
B. ファイルのハッシュをポリシーにアップロードします
C. ファイルが開くために使用していたアプリケーションをブロックします
D. 動的分析のためにファイルをCisco ThreatGridに送信します
正解: (正解を表示します)

質問: **191**
同じネットワークセグメント上のノード間の通信を個々のアプリケーションに制限するテクノロジーはどれですか？
A. マイクロセグメンテーション
B. マシンツーマシンファイアウォール
C. サーバーレスインフラストラクチャ
D. SaaSの展開
正解: (正解を表示します)

質問: **192**
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**: A (**コメントを発表する**)**
SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

質問**: 193**
進行中のフィッシングキャンペーンにより、大規模な多国籍組織のセキュリティエンジニアにとって、電子メールのセキュリティは優先度の高いタスクになっています。これを制御するために、エンジニアは、URLレピュテーションが -10 00～-600）の着信コンテンツフィルタを Cisco ESAに導入しました。フィルタに一致するメッセージ内のリンクを無効にするために、システムはどのアクションを実行しますか。
A. ScreenAction
B. 検疫
C. FilterAction
D. デファン
正解**: (**正解を表示します**)**

質問**: 194**
どのネットワーク監視ソリューションがストリームを使用し、運用データをプッシュして、アクティビティのほぼリアルタイムのビューを提供しますか？
A. SNMP
B. SMTP
C. syslog
D. モデル駆動型テレメトリ
正解**: D (**コメントを発表する**)**
The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.
Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics.

Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.

質問: **195**
Cisco AMPforEndpointsとCiscoUmbrellaRoamingClientの機能の違いは何ですか。
A. AMP for Endpointsはホスト上の悪意のあるアクティビティを停止して追跡し、UmbrellaRoamingClientはURLベースの脅威のみを追跡します。
B. AMP for Endpointsはユーザーを認証し、セグメンテーションを提供します。UmbrellaRoamingClientはVPN接続のみを許可します。
C. Umbrella Roamingクライアントはホスト上の悪意のあるアクティビティを停止して追跡し、AMPforEndpointsはURLベースの脅威のみを追跡します。
D. Umbrella Roaming Clientはユーザーを認証してセグメンテーションを提供し、AMPforEndpointsはVPN接続のみを許可します
正解: **(**正解を表示します**)**

質問: **196**
展示を参照してください。

この出力を生成し、dot1xまたはmabで認証しているポートを表示する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. 認証方法を表示
C. dot1xをすべて表示
D. 認証セッションを表示
正解: **D (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137 Displaying the Summary of All Auth Manager Sessions on the Switch Enter the following:

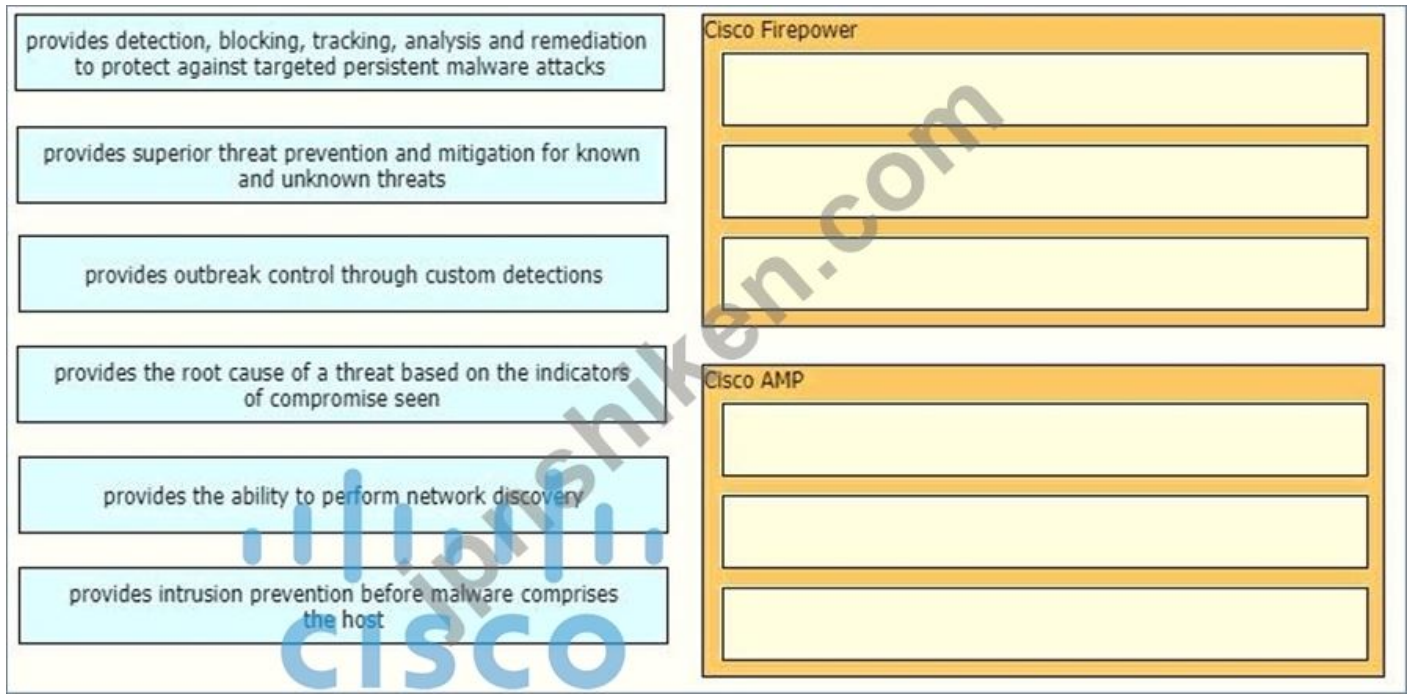
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58 Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

質問: **197**
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: **A** (コメントを発表する)
DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNS server and used to control a remote server and applications.

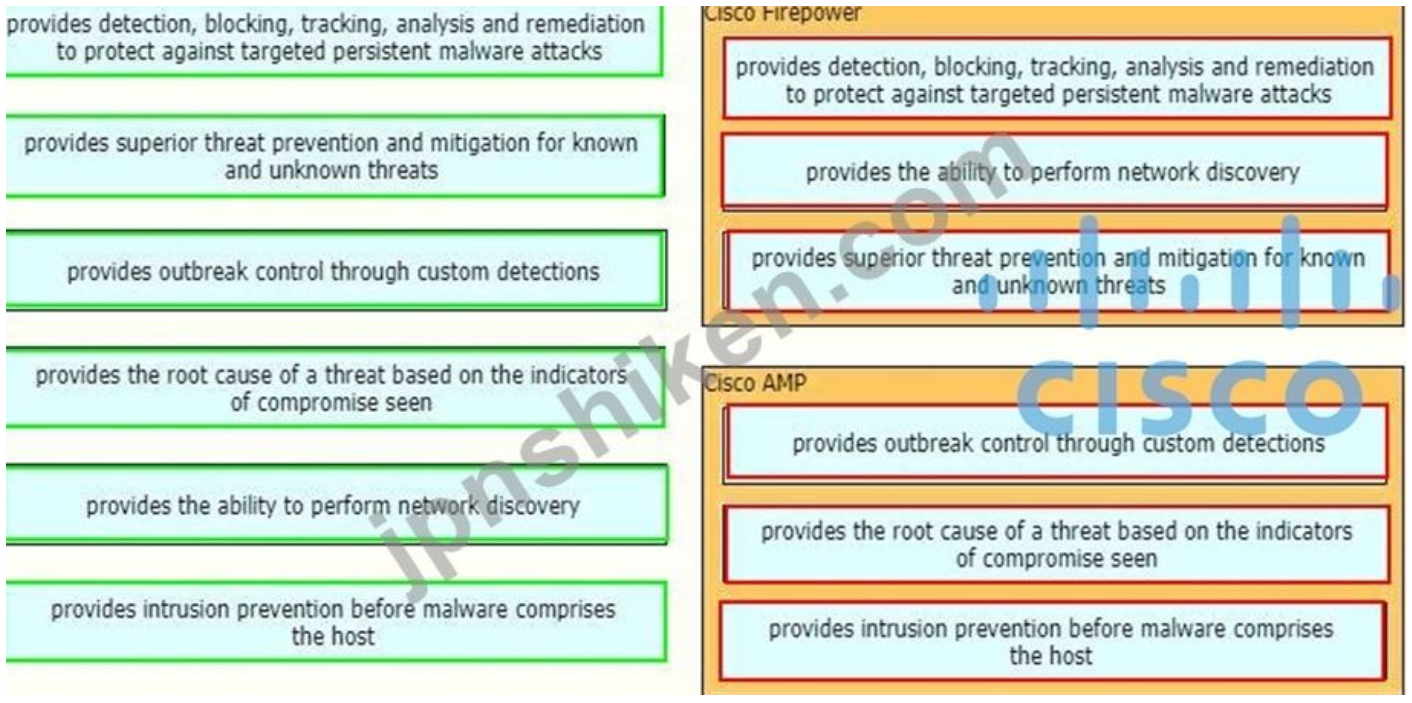
質問: **198**
管理者ログインを機能させるために、Cisco ISEでシャドウユーザーを作成する必要があるIDストアはどれですか。
A. Active Directory
B. LDAP
C. 内部データベース
D. RSA SecureID
正解: (正解を表示します)

質問: **199**
CI/CD パイプラインの概念は何ですか?
A. プロジェクトは時間制限のあるサイクルに分割され、継続的なコード レビューのためのペア プログラミングに焦点を当てています。
B. プロジェクトは複数のフェーズに分割されており、前のフェーズが正常に終了するまで 1 つのフェーズを開始できません。
C. 各プロジェクト フェーズは、適応性と継続的な改善を維持するために、他のフェーズから独立しています。
D. プロジェクト コードは一元管理されており、コードを変更するたびに自動化されたビルドとテスト シーケンスがトリガーされます。
正解: (正解を表示します)

質問: **200**
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: **201**

大学のポリシーでは、研究のためにインターネット上のリソースへのオープン アクセスを許可する必要がありますが、内部のワークステーションはマルウェアにさらされています。選択したいくつかのワークステーションにファイルがインストールされているかどうかをエンジニアリング チームが判断できる Cisco AMP の機能はどれですか?

A. ファイルの検出

B. ファイルマネージャー

C. ファイルの確信

D. ファイルの普及率

正解: **D** (コメントを発表する)

質問: **202**
展示を参照してください。
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は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はリダイレクトされます
正解: **(**正解を表示します**)**
The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces. Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces.
The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces. Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html

質問: **203**
Cisco AMP for Endpointsは、組織がマルウェアのさまざまなファミリを検出するのを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: **A (**コメントを発表する**)**
ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference:
ETHOS = Fuzzy Fingerprinting using static/passive heuristics

質問: **204**
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 public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: ...
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

質問: **205**
DevSecOpsはIT環境のどの部分に焦点を当てていますか？
A. アプリケーション開発
B. ワイヤレスネットワーク
C. データセンター
D. 境界ネットワーク
正解: **(**正解を表示します**)**

質問: **206**
DNSトンネリングはどのようにデータを盗み出しますか？
A. 攻撃者は、非標準のDNSポートを使用して、組織のDNSサーバーにアクセスし、解決策を妨害します。
B. 攻撃者は、DNSレコードに基づいてクライアントが接続するドメインを登録し、その接続を介してマルウェアを送信します。
C. 攻撃者は逆引きDNSシェルを開いてクライアントのシステムに侵入し、マルウェアをインストールします。
D. 攻撃者は、DNSリゾルバーが隠されているターゲットに電子メールを送信して、悪意のあるドメインにリダイレクトします。
正解: **B (**コメントを発表する**)**

質問: **207**
シスコや他のベンダーの複数のセキュリティ製品がデータを共有し、相互運用できるようにするために、オープンでスケーラブルなIETF標準に基づいて構築されたシスコ製品はどれですか。
A. 高度なマルウェア保護
B. プラットフォーム交換グリッド
C. マルチファクタープラットフォーム統合
D. 火力脅威防御
正解: **B (**コメントを発表する**)**
With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

質問: **208**
エンドポイント用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. exploits
B. ARP spoofing
C. denial-of-service attacks

D. malware
E. eavesdropping
正解: **(**正解を表示します**)**
Malware means "malicious software", is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.
Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.
Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.
An exploit is a code that takes advantage of a software vulnerability or security flaw.
Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

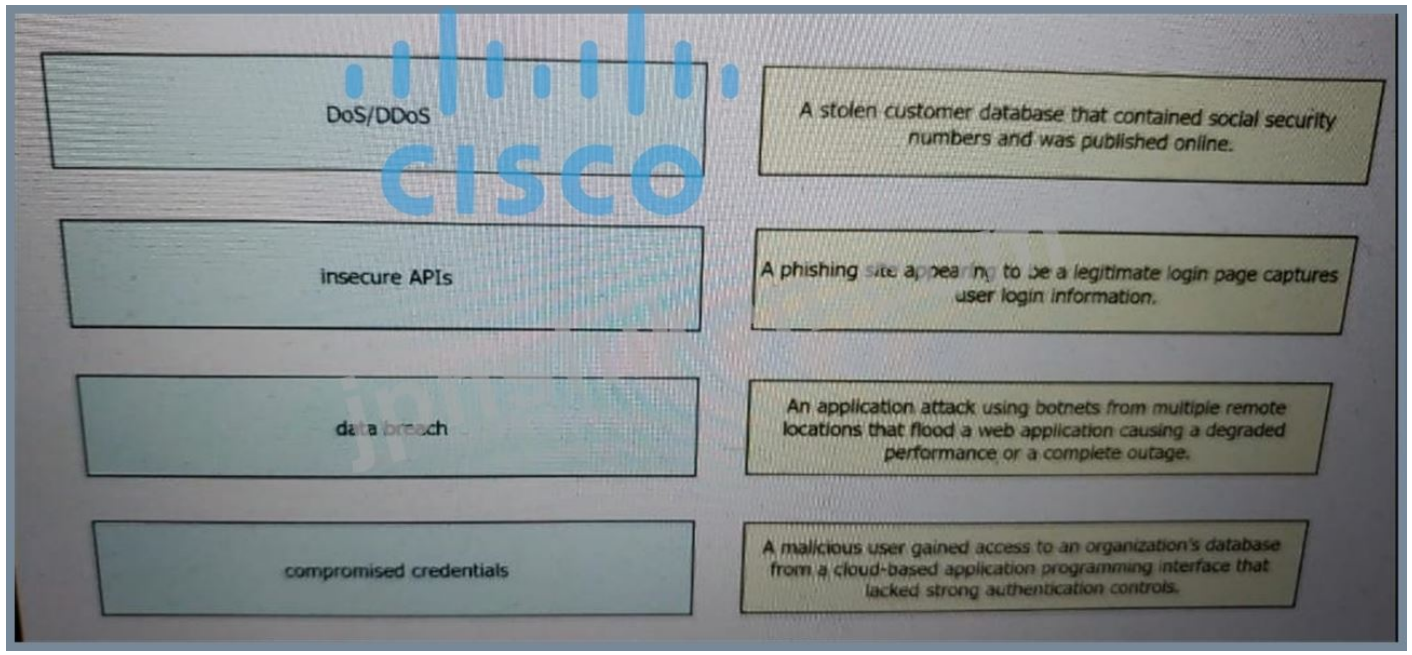
質問: **209**
CiscoFirePOWERセンサーをFirepowerManagementCenterに登録するために使用されるCLIコマンドはどれですか。
A. configure manager add <host> <key>
B. システム追加<ホスト> <キー>を構成します
C. マネージャーの削除を構成する
D. マネージャーの構成<キー>ホストの追加
正解: **(**正解を表示します**)**

質問: **210**
Cisco AMP for Endpoints管理者は、特定のMD5シグニチャを追加するようにカスタム検出ポリシーを設定します。設定は単純な検出ポリシーセクションで作成されますが、機能しません。この失敗の理由は何ですか。
A. 管理者は、CiscoAMPが使用するハッシュの代わりにファイルをアップロードする必要があります。
B. MD5シグネチャの検出は、高度なカスタム検出ポリシーで構成する必要があります
C. 検出対象のアプリケーションのAPKをアップロードする必要があります
D. 単純検出ポリシーにアップロードされたMD5ハッシュの形式が正しくありません
正解: **B (**コメントを発表する**)**

質問: **211**
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**)**
The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

Reference:
sy-book/sec-rad-coa.html

質問: 212
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: **213**
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 can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint.
NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system

質問: **214**
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. アウトバウンド
B. 東西
C. 南北
D. インバウンド
正解: **A (コメントを発表する)**

質問: **215**
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: **D (コメントを発表する)**
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.
+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).

Reference:
Note:
+ Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights.
+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a condition of an alerting policy has been met.

質問: **216**
クラウドでパッチ管理を提供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 Tetration
B. Cisco CloudLock
C. Cisco ISE
D. Cisco アンブレラ
正解: **(**正解を表示します**)**

質問: **217**
Cisco WSAのレイヤ4トラフィックモニタの機能は何ですか？
A. SSLトラフィックを復号化して、悪意のあるコンテンツを監視します
B. 悪意のあるコンテンツが含まれていることがわかっているURLカテゴリからのトラフィックをブロックします
C. 指定された機密情報をすべてのネットワークトラフィックで検索することにより、データの漏えいを防ぎます
D. すべてのTCP/UDPポートで疑わしいトラフィックを監視します
正解: **(**正解を表示します**)**

質問: **218**
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。動的ARP検査が適用された後、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. 動的ARP検査がすべてのVLANで有効になっているわけではありません
D. no ip arp Inspectiontrust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**)**
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

質問: **219**
Cisco FTDエンジニアは、組織向けにs2s00123456789という新しい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了できるようにしています。現在、ポリシーは1つしか確立されておらず、一部のデバイスが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。プライマリポリシーに記載されてい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のすべての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: **B** (コメントを発表する)
All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section. The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.
All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section. The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

質問: **220**
可視性の向上、ポリシーの統合と導入、およびアクセス リストによるセキュリティ ポリシーの実装のために、Cisco ACI を統合するのはどの VMware プラットフォームですか?
A. VMware フュージョン
B. VMwarevRealize
C. VMware APIC
D. VMware の視野
正解: (正解を表示します)

質問: **221**
Cisco Firepowerインパクトフラグの主な機能はどのオプションですか？
A. レポートで既知および疑わしい悪意のあるIPアドレスを強調表示します。
B. 侵入と脆弱性に関するデータを相互に関連付けます。
C. 重大なイベントが発生したときに管理者に警告します。
D. ASAがFirepowerモジュールに送信するデータを識別します。
正解: **B** (コメントを発表する)

質問: **222**
マイクロセグメンテーションの説明は何ですか？
A. 環境は、集中管理されたホストベースのファイアウォールルールを各サーバーまたはコンテナーに展開します。
B. 環境はゼロトラストモデルを適用し、さまざまなサーバーまたはコンテナー上のアプリケーションが通信する方法を指定します。
C. 環境は、Kubernetesなどのコンテナオーケストレーションプラットフォームをデプロイして、アプリケーションの配信を管理します。
D. 環境は、同様のアプリケーションでサーバーをグループ化するためにプライベートVLANセグメンテーションを実装します。

正解: **(**正解を表示します**)**

質問: **223**
DNSトンネリング攻撃中にデータはどのように攻撃者に送信されますか？
A. DNS応答パケットの一部として
B. ドメイン名の一部として
C. UDP'53パケットペイロードの一部として
D. TCP / 53パケットヘッダーの一部として
正解: **(**正解を表示します**)**

質問: **224**
Cisco DNA Centerのオープ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. インテントベースのAPI
C. 自動化アダプター
D. ドメイン統合
正解: **(**正解を表示します**)**

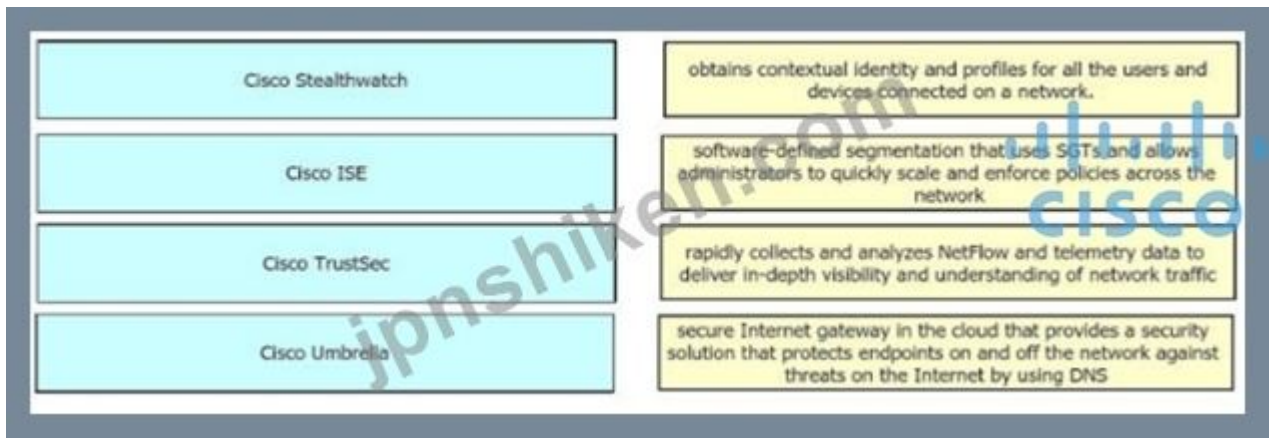
質問: **225**
組織は、サイバーセキュリティプロセスを改善し、データにインテリジェンスを追加したいと考えています。組織は、CiscoFTDおよびCiscoWSAと統合できるURLフィルタリング、レピュテーション、および脆弱性情報に最新のインテリジェンスデータを利用したいと考えています。これらの目的を達成しますか？
A. Internet StormCenterインテリジェンスフィードのシスコ FTDおよびシスコ WSAデータベースへの自動ダウンロードを作成して、動的アクセス制御ポリシーに関連付けます。
B. IETFから脅威インテリジェンスフィードをダウンロードし、CiscoFTDおよびCiscoWSAデータベースにインポートします
C. Talos Intelligenceとの統合を構成して、提供する脅威インテリジェンスを活用します。
D. NISTへのCisco pxGrid接続を作成して、ポリシーで使用するためにこの情報をセキュリティ製品にインポートします
正解: **C (**コメントを発表する**)**

質問: **226**
プロアクティブなエンドポイント保護を提供し、管理者が展開を一元管理できるようにするシスコ製品はどれですか。
A. AMP
B. WSA
C. ESA
D. NGFW
正解: **(**正解を表示します**)**

質問: **227**
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ており、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です
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、トラフィックの管理に使用されます
正解: **(**正解を表示します**)**
A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.
Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.
You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.
Reference:
Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

質問: **228**
CiscoISEのデフォルトのゲストタイプはどの役割ですか。
A. 毎月
B. 毎年
C. 請負業者
D. フルタイム
正解: **C (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/security/ise/1-4-1/admin_guide/b_ise_admin_guide_141/b_ise_admin_guide_141_chapter_01110.html

質問: **229**
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:

質問: **230**
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** (コメントを発表する)
FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco IKEv2 implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

質問: **231**
EPP と EDR の違いは何ですか?
A. EPP は主に、環境に侵入した最前線の防御を回避した脅威に焦点を当てています。
B. EPP ソリューションを使用すると、エンジニアは最新の脅威を検出、調査、修復できます。
C. EDR ソリューションを使用すると、エンジニアは、悪意のある動作の最初の兆候で問題のあるファイルにフラグを付けることができます。
D. EDR は境界での防止のみに焦点を当てています。
正解: (正解を表示します)

質問: **232**
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: **233**
エンジニアは、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するために活用できるソリューションの実装を任されています。Ciscoクラウドネイティブ CASBおよび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する必要があります。これらの要件を満たすために何を使用する必要がありますか？
A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock
正解: **D (**コメントを発表する**)**
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45- 738565.pdf

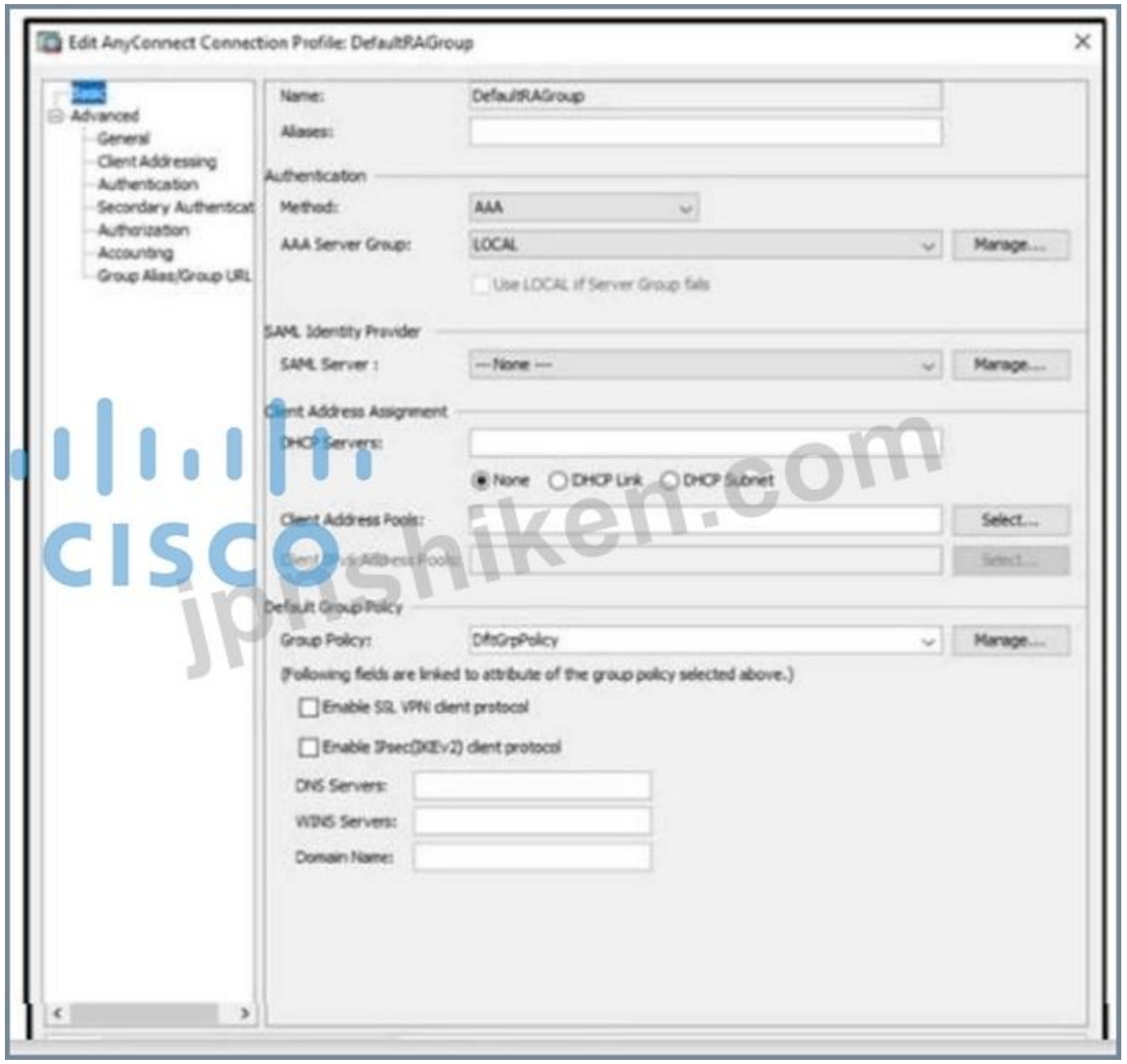
質問: **234**
エンド ユーザを Cisco WSA に対して認証するには、どの 2 つのプロトコルを設定する必要がありますか？ （2つ選んでください。）
A. TACACS+
B. ケルベロス
C. チャップ
D. 半径
E. NTLMSSP
正解: **A,D (**コメントを発表する**)**

質問: **235**
エンジニアは、CiscoUmbrella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. 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。
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. 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。
D. 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。

正解: **A** (コメントを発表する)

質問: **236**

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. メソッド

C. SAMLサーバー

D. DHCPサーバー

正解: **B** (コメントを発表する)

In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

質問: **237**

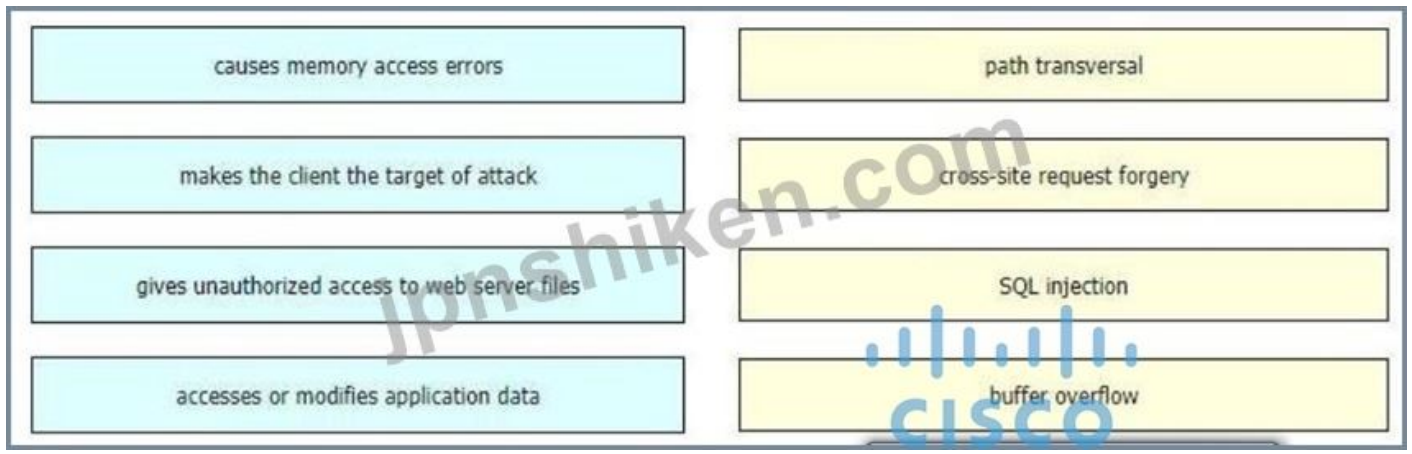
Dos攻撃が含まれるカテゴリはどれですか？
A. フィッシング攻撃
B. 洪水攻撃
C. トロイの木馬攻撃
D. ウイルス攻撃
正解: **(**正解を表示します**)**

質問: **238**
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. アプリケーション セキュリティ ゲートウェイ
B. エンドツーエンドの暗号化
C. 二要素認証
D. モジュール ポリシー フレームワーク
正解: **(**正解を表示します**)**

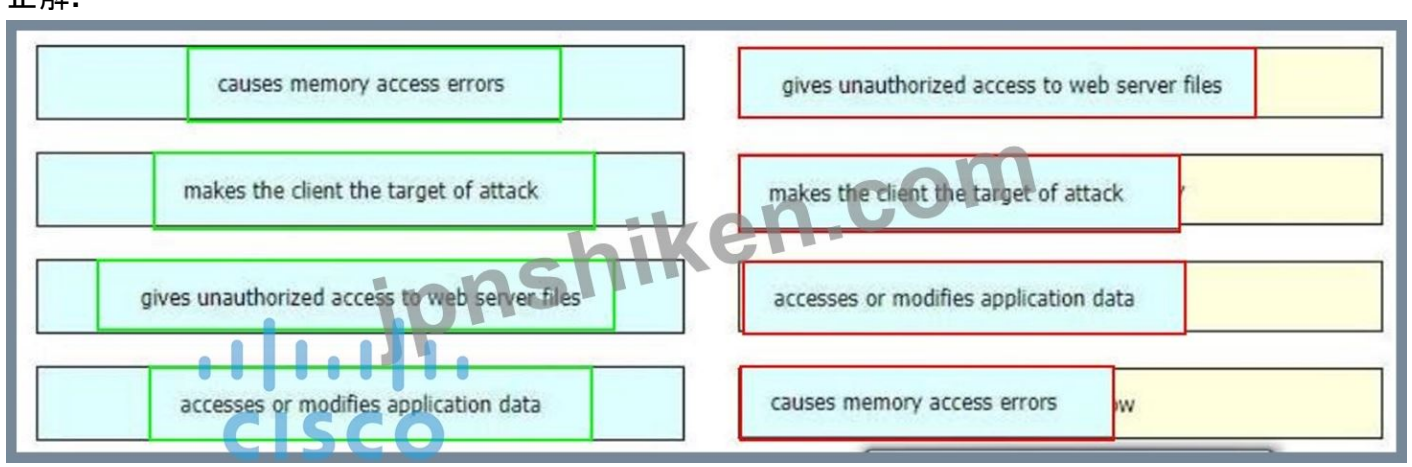
質問: **239**
Cisco FMCが他の製品からセンサーに監視可能なセキュリティインテリジェンスをプッシュできるようにする製品はどれですか？
A. コグニティブ脅威分析
B. 脅威インテリジェンスディレクター
C. 暗号化されたトラフィック分析
D. Cisco Talos Intelligence
正解: **(**正解を表示します**)**

質問: **240**
ネットワーク セキュリティ エンジニアは、問題のトラブルシューティング中に Cisco FMC Web ブラウザからパケット キャプチャをエクスポートする必要があります。アドレス https://<FMC IP>/capure/CAPI/pcap/test.pcap に移動すると、エラー 403: Forbidden が PCAP ファイルの代わりに表示されます。この問題を解決するために、エンジニアはどのアクションを実行する必要がありますか?
A. HTTPS サーバーを無効にし、代わりに HTTP を使用します。
B. ブラウザのプロキシ設定を無効にする
C. デバイス プラットフォーム ポリシーの HTTPS サーバーを有効にします。
D. ブラウザのプロキシ サーバ設定として Cisco FTD の IP アドレスを使用します。
正解: **(**正解を表示します**)**

質問: **241**
エクスプロイトを左側から右側のセキュリティ脆弱性のタイプにドラッグアンドドロップします。



正解:



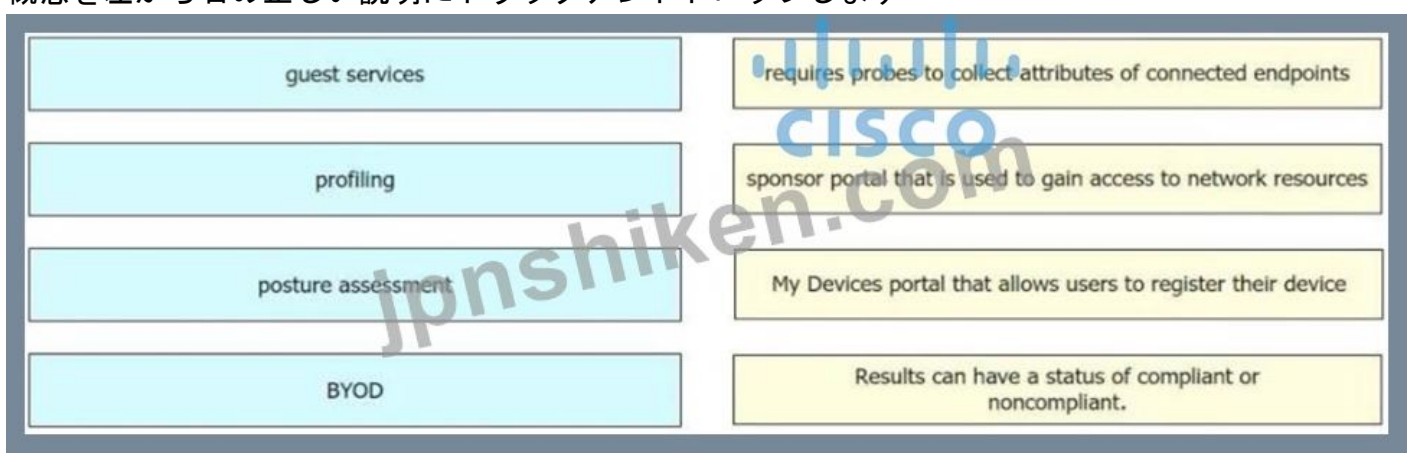
質問: **242**
基盤となるクラウドインフラストラクチャを管理または維持する必要なしに、クラウドコンシューマーがアプリケーションを開発および展開するための環境を提供するクラウドサービスモデルはどれですか？
A. Paas
B. Xaas
C. Iaas
D. Saas
正解: **(**正解を表示します**)**
Cloud computing can be broken into the following three basic models:
+ Infrastructure as a Service (IaaS): IaaS describes a cloud solution where you are renting infrastructure. You purchase virtual power to execute your software as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model because you pay for what you use.

+ Platform as a Service (PaaS): PaaS provides everything except applications. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application programming interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform.
+ Software as a Service (SaaS): SaaS is designed to provide a complete packaged solution. The software is rented out to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a peruse fee.

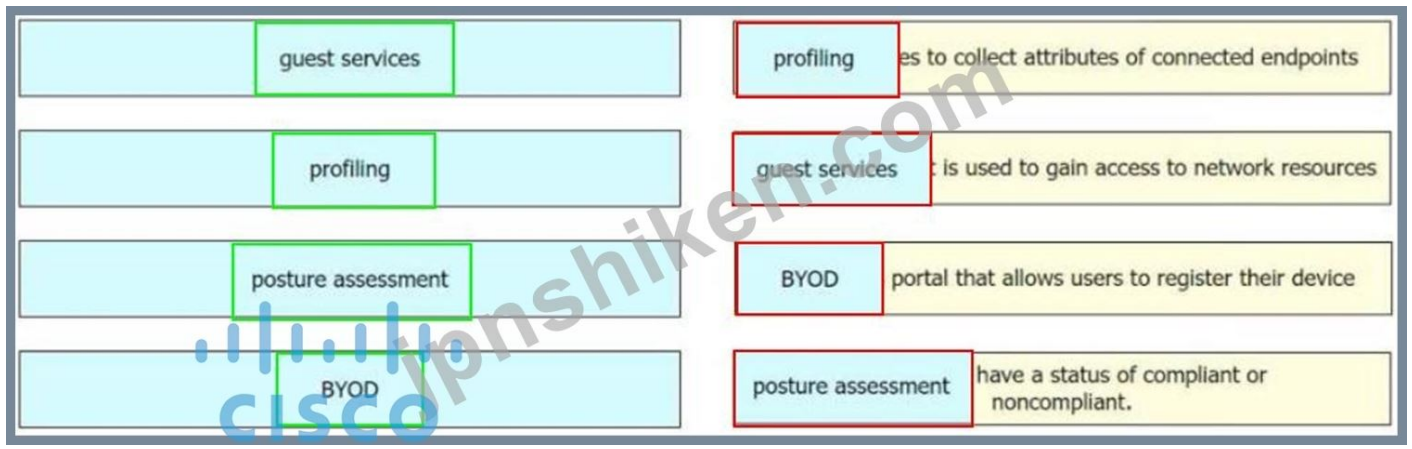
質問: **243**
大規模な組織は、パブリッククラウドにセキュリティアプライアンスを導入してサイト間VPNを形成し、パブリッククラウド環境を本社のデータセンターのプライベートクラウドにリンクしたいと考えています。これらの要件を満たすCiscoセキュリティアプライアンスはどれですか。
A. Cisco ASAV
B. Cisco Stealthwatch Cloud
C. Cisco WSAV
D. Cisco Cloud Orchestrator
正解: **(**正解を表示します**)**

質問: **244**
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CiscoAsyncOS10.0以降を実行している必要があります。
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。
正解: **D (**コメントを発表する**)**

質問: **245**
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



正解:



質問: **246**

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

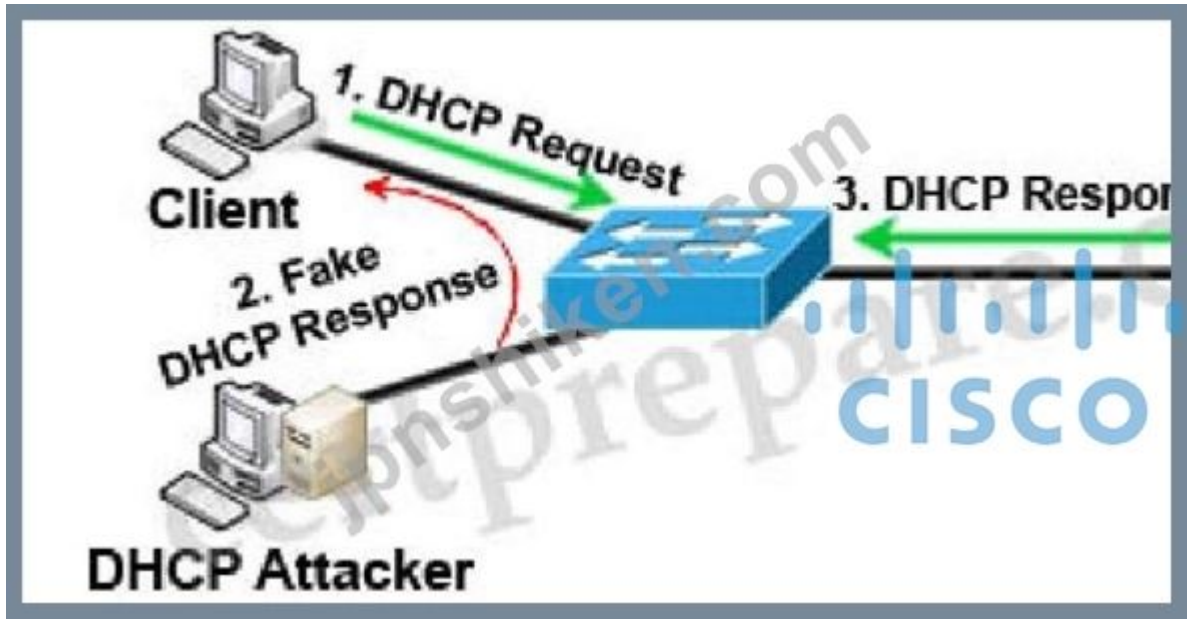
B. DHCPスヌーピングビットを1に設定します

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**)**

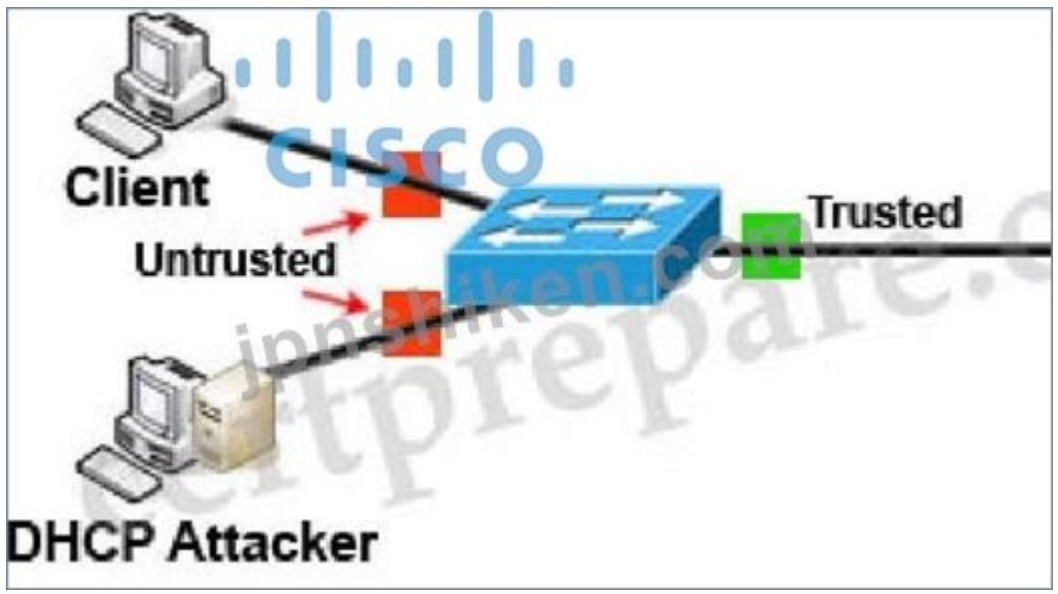
To understand DHCP snooping we need to learn about DHCP spoofing attack first.



DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.

DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.



Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

質問: **247**
付属のネイティブリモートデスクトップサポートを使用した在庫とデバイスの追跡、リモートビュー、ライブトラブルシューティングの管理など、モバイルとPCの総合的な管理を提供するものは何ですか？
A. モバイルデバイス管理
B. モバイルコンテンツ管理
C. モバイルアプリケーション管理
D. モバイルアクセス管理
正解: **(**正解を表示します**)**

質問: **248**
暗号化に関して3DESの機能は何ですか？
A. トラフィックを暗号化します。
B. 1回限りのパスワードを作成します。
C. 秘密鍵を生成します。
D. ファイルをハッシュします。
正解: **(**正解を表示します**)**

質問: **249**
管理者がプライベートクラウド管理のためにスイッチをDCNMに追加する方法を制御できるように、ファブリックにスイッチを追加するために使用する必要がある2つの方法はどれですか。（2つ選択してください。）
A. CiscoPrimeインフラストラクチャ
B. Cisco Cloud Director
C. PowerOn自動プロビジョニング
D. シードIP
E. CDP AutoDiscovery

正解: **(**正解を表示します**)**

質問: **250**
エンドポイントのパッチ適用戦略が重要なのはなぜですか？
A. パッチ適用戦略が、アプリケーションで安全でないプロトコルを無効にするのに役立つようにするため
B. 使用時に機能がより高速に向上するように
C. 既知の脆弱性を対象とし、定期的なパッチサイクルを適用することでリスクを軽減します
D. パッチでリリースされた新機能を利用する
正解: **(**正解を表示します**)**

質問: **251**
Cisco AdvancedPhishingProtectionソリューションがフィッシング攻撃から保護するために実行する2つの機能はどれですか。2つ選択してください。）
A. 電子メールメッセージが悪意があるかどうかを判断します
B. リアルタイムのユーザーWebブラウジング行動分析を行います
C. オンプレミスの電子メール展開に対する防御を提供します
D. 静的アルゴリズムを使用して悪意のあるものを特定します
E. 悪意のあるWebサイトをブロックし、ブロックリストに追加します
正解: **A,C (**コメントを発表する**)**

質問: **252**
エンドポイント保護プラットフォームとエンドポイント検出および応答の主な違いは何ですか？
A. EPPは予防に重点を置き、EDRは境界防御を回避する高度な脅威に重点を置いています。
B. EDRはネットワークセキュリティに重点を置き、EPPはデバイスセキュリティに重点を置いています。
C. EDRは予防に重点を置き、EPPは境界防御を回避する高度な脅威に重点を置いています。
D. EPPはネットワークセキュリティに重点を置き、EDRはデバイスセキュリティに重点を置いています。
正解: **(**正解を表示します**)**

質問: **253**
CiscoIOSXEデバイスでネットワークテレメトリのグラフィカルな視覚化を作成するためにシスコが使用しているオープンソースツールはどれですか。
A. SNMP
B. Grafana
C. InfluxDB
D. Splunk
正解: **(**正解を表示します**)**

質問: **254**
プラットフォームがネットワークトラフィックフロー内のさまざまなアプリケーションを識別して出力できるようにする、レイヤー3からレイヤー7の革新的なディープパケットインスペクションの利点を提供するテクノロジーはどれですか。

A. Cisco ASAV
B. Cisco Prime Infrastructure
C. Cisco NBAR2
D. 解決に関するアカウント
正解: **(**正解を表示します**)**

質問: **255**
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溢れ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 DataUnitガード
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: **C (**コメントを発表する**)**
Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.
By using the "storm-control broadcast level [falling-threshold]" we can limit the broadcast traffic on the switch.

質問: **256**
EPP と EDR の違いは何ですか?
A. EPP は主に、環境に侵入した最前線の防御を回避した脅威に焦点を当てています。
B. EPP ソリューションを使用すると、エンジニアは最新の脅威を検出、調査、修復できます。
C. EDR ソリューションを使用すると、エンジニアは、悪意のある動作の最初の兆候で問題のあるファイルにフラグを付けることができます。
D. EDR は境界での防止のみに焦点を当てています。
正解: **B (**コメントを発表する**)**

質問: **257**
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. ファイルレピュテーションセンター
B. IPおよびドメインレピュテーションセンター
C. AMPレピュテーションセンター

D. IPブラックリストセンター
正解: **B** (コメントを発表する)

質問: **258**
Cisco エンドポイント IoC 機能の目的は何ですか?
A. インシデント対応ツールです。
B. ステルス脅威の防止を提供します。
C. 署名ベースのエンジンです。
D. 事前侵害検出を提供します。
正解: **A** (コメントを発表する)
Reference:
The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

質問: **259**
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. 高度なポリシーを適用します。
C. 次の識別プロファイルポリシーを適用します。
D. リクエストをブロックします。
正解: (正解を表示します)

質問: **260**
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)
In this IaaS model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices.
Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

質問: **261**
Cisco DNA Centerのどの2つの機能が、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ますか。 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 (コメントを発表する**)**
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours. Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent. Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes. Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours.
Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent.
Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes.
Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices.
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours. Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent. Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data

sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes. Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html

質問: **262**
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 devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference:
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.

質問: **263**
管理者はCiscoISE内で新しい許可ポリシーを設定し、デバイスのプロファイリングに問題があります。RADIUS認証に基づいてプロファイリングされた新しいCiscoIP Phoneの属性は表示されますが、CDPまたはDHCPの属性は表示されません。この問題に対処するには、管理者は何をする必要がありますか？
A. DHCPインターフェイスでip dhcp snooping trustコマンドを設定して、CiscoISEに情報を取得します。
B. Cisco ISE内で認証ポート制御自動機能を設定して、接続しようとしているデバイスを識別します
C. スイッチ内でサービステンプレートを設定して、ポート設定を標準化し、正しい情報がCiscoISEに送信されるようにします。
D. 適切なプロトコル情報を送信するようにスイッチ内のデバイスセンサー機能を構成します
正解: **(**正解を表示します**)**
Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols:
+ Cisco Discovery Protocol (CDP)
+ Link Layer Discovery Protocol (LLDP)
+ Dynamic Host Configuration Protocol (DHCP)

質問: **264**
パブリック クラウド、プライベート クラウド、ハイブリッド クラウド、およびコミュニティ クラウドを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 pxGrid

B. Cisco ASAv
C. Cisco ISE
D. Cisco Cloudlock
正解: **(**正解を表示します**)**

質問: **265**
展示を参照してください。

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

構成で使用されている認証プロトコルに関する説明として正しいものはどれですか。
A. 認証リクエストにはパスワードのみが含まれています
B. 認証リクエストにはユーザー名のみが含まれます
C. 認証と承認のリクエストは1つのパケットにグループ化されます
D. 認証と承認のリクエストパケットが別々にあります
正解: **(**正解を表示します**)**
This command uses RADIUS which combines authentication and authorization in one function (packet).

質問: **266**
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
B. 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であるかブロードキャストであるかを判別します。
C. トラフィックストーム制御は、合計トラフィックが間隔内のレベルを超えると、すべてのブロードキャストトラフィックとマルチキャストトラフィックをドロップします
D. 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。
正解: **C (**コメントを発表する**)**

質問: **267**
展示を参照してください。

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```


https://api.amp.cisco.com/v1/computersでの作業中にAPIキーは何をしますか？
A. HTTP認証
B. クライアントIDを表示します
C. HTTP認証

D. リクエストをインポートします
正解: **A** (コメントを発表する)

質問: **268**
AMP for Endpoints コンソールで、エンドポイントで特定の MD5 シグニチャを検出し、ファイルを隔離するために実行する必要があるアクションはどれですか?
A. シンプルなカスタム検出リストを構成する
B. 高度なカスタム検出リストを構成します。
C. アプリケーションのカスタム検出リストを構成する
D. IP ブロックと許可のカスタム検出リストを構成する
正解: (正解を表示します)