Cisco.350-701J.v2022-09-26.q154

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： 154
バージョン： v2022-09-26
ページの閲覧量： 503
問題集の閲覧量： 8836
https://www.jpnshiken.com/shiken/Cisco.350-701J.v2022-09-26.q154.html

質問: **1**
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 WSAV
B. Cisco Stealthwatch Cloud
C. Cisco Cloud Orchestrator
D. Cisco ASAV
正解: **D (**コメントを発表する**)**

質問: **2**
CiscoSDNアーキテクチャ内のノースバウンドAPIとサウスバウンドAPIの2つの機能は何ですか。2つ選択してください。）
A. サウスバウンドAPIは、SDNコントローラーをアプリケーションと統合する方法を定義するために使用されます。
B. ノースバウンドインターフェイスは、OpenFlowとOpFlexを利用してネットワークデバイスと統合します。
C. ノースバウンドAPIは、GET、POST、DELETEなどのRESTfulAPIメソッドを利用します。
D. サウスバウンドインターフェースは、VLANやIPアドレスなどのデバイス構成を利用します。
E. サウスバウンドAPIは、CLI、SNMP、およびRESTCONFを利用します。
正解: **(**正解を表示します**)**

質問: **3**
Cisco Firepower管理者は、ネットワーク上でこれまでに見たことのない新しいアプリケーションを許可するようにルールを設定する必要があります。トラフィックが検査なしで通過できるようにするには、どの2つのアクションを選択する必要がありますか？　2つ選択してください。）
A. 許可
B. 信頼
C. リセット
D. 許可する
E. モニター

正解: **B,E** (コメントを発表する)
Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.
Note: With action "trust", Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

質問: **4**
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: **5**
NetFlowセキュアイベントロギングの機能は何ですか？
A. v5およびv8テンプレートをサポートします。
B. 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。
C. 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。
D. 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。
正解: (正解を表示します)

質問: **6**
組織の環境にCiscoStealthwatchCloudが導入されています。クラウドロギングは期待どおりに機能していますが、オンプレミスネットワークからログが受信されていません。この問題を解決するには、どのようなアクションを実行しますか？
A. syslogをCisco StealthwatchCloudに送信するようにセキュリティアプライアンスを設定します
B. NetFlowをCisco StealthwatchCloudに送信するようにセキュリティアプライアンスを設定します
C. Cisco FTDセンサーを導入して、イベントをCisco StealthwatchCloudに送信します
D. ネットワークにCisco Stealthwatch Cloudセンサーを導入して、Cisco StealthwatchCloudにデータを送信します
正解: (正解を表示します)
You can also monitor on-premises networks in your organizations using Cisco Stealthwatch Cloud. In order to do so, you need to deploy at least one Cisco Stealthwatch Cloud Sensor appliance (virtual or physical appliance).

質問: **7**
Cisco SecurityIntelligenceがCiscoNext Generation Intrusion Prevention Systemで機能するには、どのライセンスが必要ですか。
A. マルウェア
B. コントロール
C. 保護する

D. URLフィルタリング
正解: **(**正解を表示します**)**

質問: **8**
SDNノースバウンドAPIの2つの機能は何ですか？ 2つ選択してください。）
A. OpenFlowは標準化されたノースバウンドAPIプロトコルです。
B. ノースバウンドAPIは、SDNコントローラーとビジネスアプリケーション間のインターフェイスを形成します。
C. ノースバウンドAPIは、SDNコントローラーとネットワークスイッチまたはルーター間のインターフェイスを形成します。
D. ノースバウンドAPIは、NETCONFプロトコルを使用してアプリケーションと通信します。
E. ノースバウンドAPIは、アプリケーションがネットワークを動的に構成するためのプログラム可能なインターフェースを提供します。
正解: **(**正解を表示します**)**

質問: **9**
Cisco ESAでは防止できるがCiscoWSAでは防止できない攻撃はどれですか。
A. バッファオーバーフロー
B. DoS
C. SQLインジェクション
D. フィッシング
正解: **D (**コメントを発表する**)**
The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway: Prevents the following: + Attacks that use compromised accounts and social engineering. + Phishing, ransomware, zero-day attacks and spoofing. + BEC with no malicious payload or URL. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html Gateway:
Prevents the following:
+ Attacks that use compromised accounts and social engineering.
+ Phishing, ransomware, zero-day attacks and spoofing.
+ BEC with no malicious payload or URL.
Reference:
The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway: Prevents the following: + Attacks that use compromised accounts and social engineering. + Phishing, ransomware, zero-day attacks and spoofing. + BEC with no malicious payload or URL. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

質問: **10**
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. ActiveDirectoryグループポリシーを使用してCiscoUmbrellaDNSサーバーを適用する
B. CiscoUmbrellaローミングクライアントを使用する
C. 企業のネームサーバーにDNSクエリを強制する
D. DNSルックアップのレジストリを変更する
正解: **(**正解を表示します**)**

質問: **11**
AESに有効な2つのキーとブロックのサイズはどれですか？ （2つ選択してください。）
A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length
正解: **(**正解を表示します**)**
The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

質問: **12**
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: **B (**コメントを発表する**)**
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: **13**
エンジニアは、デフォルトのアクションを使用せずに常に検査のためにトラフィックを送信するようにアクセス制御ポリシールールを構成する必要があります。このルールに対してどのアクションを構成する必要がありますか？
A. 許可する
B. モニター
C. ブロック
D. 信頼
正解: **(**正解を表示します**)**

質問: **14**

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: **15**
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: **16**
Cisco Umbrellaはどのようにログを企業所有のストレージにアーカイブしますか？
A. アプリケーションプログラミングインターフェイスを使用してログを取得する
B. syslogを介してオンプレミスまたはクラウドベースのsyslogサーバーにログを送信する
C. システム管理者がCisco UmbrellaWebポータルからログをダウンロードする
D. 自己管理型AWSS3バケットにログを送信するように設定する
正解: **D (**コメントを発表する**)**
The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket. By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage. Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.
The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket. By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage. Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs

質問: **17**
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). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf 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).
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). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf

質問: **18**
エンジニアは、ルーターの構成が侵害された場合に資格情報が表示されないようにするために、ルーターでデバイス強化を構成しています。どのコマンドを使用する必要がありますか？
A. サービスパスワード回復
B. ユーザー名<ユーザー名>パスワード<パスワード>
C. サービスパスワード暗号化
D. ユーザー名<ユーザー名>特権15パスワード<パスワード>
正解: **(**正解を表示します**)**

質問: **19**
Cisco ASA5500シリーズファイアウォールでNetFlowを許可する2つのタスクはどれですか。 2つ選択してください）

A. NetFlowExporterをインバウンド方向の外部インターフェイスに適用します。
B. NetFlowバージョン9を有効にします。
C. ポート9996でUDPトラフィックを許可するACLを作成します。
D. 興味深いトラフィックに一致するクラスマップを作成します。
E. flow-exportコマンドを使用してNetFlowコレクターを定義します
正解: **(**正解を表示します**)**

質問: **20**
展示を参照してください。
管理者が新しいCiscoFTDデバイスをネットワークに追加していて、CiscoFMCで管理したいと考えています。
CiscoFTDはNATデバイスの背後にありません。Cisco FTDでこれを有効にするには、どのコマンドが必要ですか。
A. configure manager add DONTRESOLVE kregistration key>
B. configure manager add <FMC IP address> <registration key> 16
C. configure manager add DONTRESOLVE <登録キー> FTD123
D. configure manager add <FMC IP address> <registration key>
正解: **(**正解を表示します**)**
To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.
Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/ choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.
To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.
Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/

質問: **21**
脅威インテリジェンスをマシンで消化可能な形式で共有するためのフレームワークを作成するオープンスタンダードはどれですか？
A. OpenIOC
B. CybOX
C. OpenC2
D. STIX
正解: **(**正解を表示します**)**

質問: **22**
DMVPNを介したCiscoAny接続を使用する2つの利点は何ですか。 （2つ選択してください。）
A. 複数のサイトがデータセンターに接続できるようにします
B. マシンからの個々のユーザーのVPNアクセスを可能にします

C. さまざまなルーティングプロトコルがトンネル上で機能できるようにします
D. ハブを通過せずにスポークツースポーク通信を提供します
E. ユーザーIDに基づいてアクセスポリシーをカスタマイズできます
正解: **(**正解を表示します**)**

質問: **23**
ハイブリッド電子メールソリューションを展開するときに、オンプレミス機器として残しておく必要がある2つのサービスはどれですか。 2つ選択してください。）
A. DDoS
B. スパム対策
C. ウイルス対策
D. 暗号化
E. DLP
正解: **(**正解を表示します**)**
Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies. Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies.
Reference:
Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies. Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

質問: **24**
エンドポイントセキュリティは、組織の全体的なセキュリティ体制にどのようなメリットをもたらしますか？
A. 組織は、境界セキュリティデバイスが検出しない脅威を検出して軽減できます。
B. ユーザーがドメインでアクティブである限り、組織はWebベースの攻撃を軽減できます
C. インシデント対応プロセスを合理化して、エンドポイントでデジタルフォレンジックを自動的に実行します
D. 組織がネットワークのエッジで脅威を検出して対応できるようにします
正解: **A (**コメントを発表する**)**

質問: **25**

PaaSモデルでは、テナントが保守とパッチ適用を担当するのはどのレイヤーですか？
A. アプリケーション
B. ハイパーバイザー
C. 仮想マシン
D. ネットワーク
正解: **(**正解を表示します**)**

質問: **26**
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: **27**
Cisco Advanced Phishing Protectionはどのようにユーザを保護しますか？
A. DKIMを使用して送信者を検証します。
B. 送信者がどのIDを認識するかを決定します
C. メッセージを安全に送信するセンサーを利用しています。
D. 機械学習とリアルタイムの行動分析を使用します。
正解: **(**正解を表示します**)**
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats. Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats. Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection

質問: **28**
コンテナオーケストレーションの機能は何ですか？
A. CiscoContainerPlatformデータプレーンを使用してAmazonECSクラスターをデプロイする機能

B. エアギャップサイトにKubernetesクラスターをデプロイする機能
C. 自動化された毎日の更新
D. CiscoContainerPlatformデータプレーンを使用してAmazonEKSクラスターをデプロイする機能
正解**: B (**コメントを発表する**)**

質問**: 29**
組織は、クラウド内のユーザー、データ、およびアプリケーションを保護したいと考えています。ソリューションはAPIベースであり、クラウドネイティブCASBとして動作する必要があります。この実装にはどのソリューションを使用する必要がありますか？
A. Cisco Cloudlock
B. Cisco Cloud Email Security
C. CiscoFirepower次世代ファイアウォール
D. Cisco Umbrella
正解**: (**正解を表示します**)**
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
Broker (CASB) and cloud cybersecurity platform.
Reference:
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**: 30**
組織がCiscoUmbrellaを使用してURLブロッキングを実装しています
a。ユーザーはいくつかのサイトに行くことができます
しかし、エラーのために他のサイトにアクセスできません。エラーが発生するのはなぜですか？
A. クライアントコンピュータにCisco Umbrella RootCA証明書がインストールされていません。
B. IP層の強制が構成されていません。
C. クライアントコンピューターには、内部CAサーバーから展開されたSSL証明書がありません。
D. インテリジェントプロキシとSSL復号化がポリシーで無効になっている
正解**: A (**コメントを発表する**)**
Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves: Custom URL Blocking-Required to block the HTTPS version of a URL. ... Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you

may wish to prevent it from appearing. To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin. Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information certificate. Having the SSL Decryption feature improves:
Custom URL Blocking-Required to block the HTTPS version of a URL.
...
Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing.
To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin.
Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves: Custom URL Blocking-Required to block the HTTPS version of a URL. ... Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing. To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin. Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information

質問**: 31**
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**: B (**コメントを発表する**)**
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: **32**
ネットワークリソースにアクセスするために、証明書を展開し、モバイルデバイスにサプリカントを構成するために使用される方法はどれですか？
A. 搭乗中のBYOD
B. 単純な証明書登録プロトコル
C. クライアントプロビジョニング
D. MAC認証バイパス
正解: **A (**コメントを発表する**)**
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices. Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.
Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.
Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.
Reference:
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices. Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html

質問: **33**
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. Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4 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. Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4

質問: **34**
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. サーバーレスインフラストラクチャ
C. マシンツーマシンファイアウォール
D. SaaSの展開
正解: **A (**コメントを発表する**)**

質問: **35**
ソフトウェアの脆弱性検出を実行しながら、動作のベースラインを処理し、逸脱を監視し、データセンターのトラフィックとサーバーの悪意のあるプロセスを確認するシスコプラットフォームはどれですか。
A. Cisco Tetration
B. Cisco AnyConnect
C. Cisco AMP for Network
D. Cisco ISE？
正解: **(**正解を表示します**)**

質問: **36**
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: **C,D (**コメントを発表する**)**

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: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/ modules-sfr.html You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference:
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: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/ modules-sfr.html

質問: **37**
脅威インテリジェンス共有におけるTAXIIの2つの機能は何ですか？ 2つ選択してください。）
A. ユーザーが脅威の動機と能力を説明できるようにします
B. 脅威インテリジェンスの 何」を決定します
C. 脅威インテリジェンス情報の中継方法を決定します
D. STIX情報をサポートします
E. 信頼できる異常インテリジェンス情報を交換します
正解: **D,E (**コメントを発表する**)**

質問: **38**
CiscoASA用のCiscoNetFlowセキュアイベントロギングの機能は何ですか。
A. 複数のNetFlowコレクターがサポートされています
B. 高度なNetFlowv9テンプレートとレガシーv5フォーマットがサポートされています
C. セキュアNetFlow接続はCisco PrimeInfrastructure用に最適化されています
D. フロー作成イベントが遅れる
正解: **(**正解を表示します**)**
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... - Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf
...
- Delays the export of flow-create events.
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... - Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf

質問: **39**
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: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero 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.
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 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: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero 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**: 40**
DMVPNはGETVPNよりもどのようなメリットがありますか？
A. 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。
B. 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。
C. DMVPNはトンネルレスVPNであり、GETVPNはトンネルベースです。
D. 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。
正解**: (**正解を表示します**)**

質問**: 41**
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**: (**正解を表示します**)**
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: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/ white-paper-c11-736595.html 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:
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: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/ white-paper-c11-736595.html

質問**: 42**
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**: (**正解を表示します**)**
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. Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide 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.
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. Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

質問: **43**
Cisco FMCが他の製品からセンサーに監視可能なセキュリティインテリジェンスをプッシュできるようにする製品はどれですか？
A. 暗号化されたトラフィック分析
B. 脅威インテリジェンスディレクター
C. コグニティブ脅威分析
D. Cisco Talos Intelligence
正解: **(**正解を表示します**)**

質問: **44**
管理者は、既存の展開に新しいCiscoISEノードを追加しています。FQDNを入力するときにノードの追加が成功するようにするには、何をする必要がありますか？
A. 新しいCiscoISEノードのDNSエントリをDNSサーバーに追加します
B. 新しいCiscoISEノードのIPアドレスを他のノードと同じネットワークに変更します。
C. プライマリに登録する前に、新しいCiscoISEノードをセカンダリPANにします。
D. CiscoISEノード間のファイアウォールでポート8905を開きます
正解: **(**正解を表示します**)**

質問: **45**
エンドポイントに一貫してパッチを適用することが重要なのはなぜですか？
A. ベンダー契約ごとにパッチが必要です。
B. パッチを適用すると、ハニーポットを作成できます。
C. パッチは脆弱性を軽減するのに役立ちます。
D. パッチを適用すると、インフラストラクチャの攻撃対象領域が減少します。
正解: **(**正解を表示します**)**

質問: **46**
Cisco Umbrella内のどの機能が、安全なHTTPトラフィックを検査する機能を可能にしますか？
A. ファイル分析
B. セーフサーチ
C. SSL復号化
D. 宛先リスト
正解: **(**正解を表示します**)**
SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root

certificate be installed. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

質問: **47**
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. 透過モード
B. ブリッジモード
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: **48**
ウイルスやマルウェアと戦うための多層アプローチでCiscoESAを構成するために使用される2つの機能はどれですか。
（2つ選択してください）
A. アウトブレイクフィルター
B. DLP
C. ソフォスエンジン
D. ホワイトリスト
E. RAT
正解: **A,C (**コメントを発表する**)**

質問: **49**
CI / CDパイプラインへの安全なアクセスのためにどのソリューションを活用する必要がありますか？
A. CiscoFTDネットワークゲートウェイ
B. リモートアクセスクライアント
C. SSL WebVPN
D. Duo Network Gateway
正解: **(**正解を表示します**)**

質問: **50**
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. ヘルスモニタリング
B. URLフィルタリング
C. 影響フラグ
D. セキュリティインテリジェンス
正解: **(**正解を表示します**)**

質問: **51**
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。
B. 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。
C. 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。
D. 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。
E. 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。
正解: **B,C (**コメントを発表する**)**

質問: **52**
有線802.1X認証を実装する場合、どの2つのコンポーネントが必要ですか？ 2つ選択してください。）
A. 認証サーバ :Cisco Prime Infrastructure
B. 認証サーバ :Cisco Identity Service Engine
C. オーセンティケータ :CiscoCatalystスイッチ
D. オーセンティケータ :Cisco Identity Services Engine
E. サプリカント :Cisco AnyConnectISEポスチャモジュール
正解: **B,C (**コメントを発表する**)**

質問: **53**
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: **(**正解を表示します**)**
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: **54**
死の攻撃のpingを特徴付ける2つの行動パターンはどれですか？ 2つ選択してください。）
A. 攻撃は送信前に16オクテットのグループに断片化されます。
B. 攻撃は送信前に8オクテットのグループに断片化されます
C. トラフィックの短い同期バーストは、TCP接続を中断するために使用されます。
D. 不正な形式のパケットがシステムのクラッシュに使用されます
E. 一般にアクセス可能なDNSサーバーは、通常、攻撃を実行するために使用されます
正解: **B,D (**コメントを発表する**)**
Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.
A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

質問: **55**
多要素認証戦略を使用する利点は何ですか？
A. 複数のアプリケーションに対して簡単なシングルサインオンエクスペリエンスを提供します
B. アプリケーションに安全なリモートアクセスを提供します。
C. IDの2番目の検証の使用を有効にすることにより、データを保護します。
D. デバイスの信頼を確立するためにデバイスを可視化します。
正解: **(**正解を表示します**)**

質問: **56**
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) Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor-for-ISE-Profilin.html 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)
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) Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor-for-ISE-Profilin.html

質問: **57**
ICMPはどのように抽出技術を使用していますか？
A. IPブロードキャストアドレスを使用して、ターゲットホストの送信元IPアドレスで多数のICMPパケットを送信する
B. 宛先ホストを到達不能なパケットでフラッディングする
C. 対象のホストをICMPエコー要求パケットで圧倒する
D. ICMPパケットのペイロードを暗号化して、侵害されたホストでコマンドおよび制御タスクを実行する
正解: **(**正解を表示します**)**

質問: **58**
組織は、短期間に大量のSPAMメッセージを受信しました。メッセージに対してアクションを実行するには、メッセージがどれほど有害であるかを判断する必要があり、これは動的に発生する必要があります。
これを実現するには何を構成する必要がありますか？
A. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoWSAを設定します。
B. Talosからリアルタイムの更新を受信するようにCiscoESAを設定します
C. Talosからリアルタイムの更新を受信するようにCiscoWSAを設定します。
D. 表示されたトラフィックに基づいてポリシーを変更するようにCiscoESAを設定します。
正解: **D (**コメントを発表する**)**
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.

質問: **59**
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. 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。
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. 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。
D. 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
E. 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。
正解: **(**正解を表示します**)**

質問: **60**
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: **(**正解を表示します**)**
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**: 61**
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. ブラウザWGET
C. バッファオーバーフロー
D. クロスサイトスクリプティング
正解**: (**正解を表示します**)**

質問: **62**
クラウドPaaSモデルのどの2つの側面が、プロバイダーではなく顧客によって管理されていますか？　2つ選択してください。）
A. 仮想化
B. ミドルウェア
C. オペレーティングシステム
D. アプリケーション
E. データ
正解: **(**正解を表示します**)**
Customers must manage applications and data in PaaS.

質問: **63**
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、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。
B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **64**
どのエンドポイント保護および検出機能が、アクティブな違反の可能性としてフラグが立てられたテレメトリ、ファイル、および侵入イベントの相関を実行しますか？
A. 侵入の痕跡
B. ファイルの軌跡
C. 遡及的検出
D. Elastic Search
正解: **(**正解を表示します**)**

質問: **65**
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: **66**
コンテンツセキュリティに使用されるAPIはどれですか？
A. OpenVuln API
B. AsyncOS API
C. NX-OS API
D. IOS XR API
正解: **(**正解を表示します**)**

質問: **67**
SDNアーキテクチャのどの機能が通信を可能にするためにサウスバウンドAPIを必要としますか？
A. SDNコントローラーとネットワーク要素
B. 管理コンソールとSDNコントローラー
C. 管理コンソールとクラウド
D. SDNコントローラーとクラウド
正解: **(**正解を表示します**)**
The Southbound API is used to communicate between Controllers and network devices

質問: **68**
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. 相関ポリシー
B. 健康意識の方針
C. 健康政策
D. システムポリシー
E. アクセス制御ポリシー

正解: (正解を表示します)

質問: **69**
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: (正解を表示します)
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: **70**
ゲストサービスのISEへの認証のためにユーザーをWebポータルにリダイレクトするために使用される2つのメカニズムは何ですか？
（2つ選択してください）
A. multiple factor auth
B. central web auth
C. TACACS+
D. local web auth
E. single sign-on
正解: **(正解を表示します)**

質問: **71**
任意から任意のスケーラブルな接続を備えたプライベートIPクラウドを介して会社の支店間で安全なVPN接続を実装するには、どのテクノロジーを使用する必要がありますか？
A. DMVPN
B. FlexVPN
C. IPsec DVTI

D. VPNを取得
正解: **(**正解を表示します**)**
Cisco's Group Encrypted Transport VPN (GETVPN) introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members (GMs) share a common security association (SA), also known as a group SA. This enables GMs to decrypt traffic that was encrypted by any other GM.
GETVPN provides instantaneous large-scale any-to-any IP connectivity using a group IPsec security paradigm.
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_2_0_External.pdf

質問: **72**
エンジニアは、pxGridを使用してCiscoFMCとCiscoISEを統合します。CiscoFMCにはどの役割が割り当てられていますか。
A. client
B. server
C. controller
D. publisher
正解: **D (**コメントを発表する**)**

質問: **73**
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: **74**
Cisco Next Generation Intrusion Prevention Systemで有効な抑制タイプはどれですか。
A. ポート
B. 出典
C. アプリケーション
D. プロトコル

E. ルール
正解: **(**正解を表示します**)**

質問: **75**
RADIUS CoA機能でサポートされているIETF属性はどれですか？
A. 30 Calling-Station-ID
B. 42 Acct-Session-ID
C. 24 State
D. 81メッセージオーセンティケーター
正解: **(**正解を表示します**)**

質問: **76**
Cisco WSAは、Webアプリケーションに帯域幅制限をどのように適用しますか。
A. アプリケーショントラフィックを低帯域幅リンクにリダイレクトするためのポリシールートを実装します。
B. スカベンジャークラスのQoSポリシーを動的に作成し、WSAを介して接続する各クライアントに適用します。
C. アプリケーショントラフィックにトラフィックポリシングを適用するコマンドをアップリンクルータに送信します。
D. アプリケーショントラフィックに遅延を導入することにより、低速のリンクをシミュレートします。
正解: **(**正解を表示します**)**

質問: **77**
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. 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。
B. 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
C. インターフェース構成にmabを追加します。
D. 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。
正解: **(**正解を表示します**)**

質問: **78**
ネットワーク管理者は、ネットワーク上に現在存在する資産を確認する必要があります。サードパーティシステムは、ホストデータをCiscoFirepowerにフィードできる必要があります。これを実現するには何を構成する必要がありますか？
A. ホストからデータを受信するためのネットワーク検出ポリシー
B. ホストからデータをダウンロードするための脅威インテリジェンスポリシー
C. ファイルデータをCiscoFirepowerに送信するためのファイル分析ポリシー
D. ホストからNetFlowデータを受信するためのネットワーク分析ポリシー
正解: **(**正解を表示します**)**
You can configure discovery rules to tailor the discovery of host and application data to your needs.
The Firepower System can use data from NetFlow exporters to generate connection and discovery events, and to add host and application data to the network map.
A network analysis policy governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt -> Answer D is not correct.

質問: **79**
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: **(**正解を表示します**)**
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: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html 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.
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 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: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html 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: **80**
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. パッチでリリースされた新機能を利用する
B. 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
C. 使用時に機能がより高速に向上するように
D. 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
正解: **D (**コメントを発表する**)**

質問: **81**
CiscoFirepowerがCiscoTalosから脅威インテリジェンスアップデートをダウンロードするタイミングを表す用語はどれですか。
A. 消費
B. 共有
C. 分析
D. オーサリング
正解: **(**正解を表示します**)**
... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector
... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

質問: **82**
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. 解決に関するアカウント
B. Cisco Prime Infrastructure
C. Cisco ASAV
D. Cisco NBAR2
正解: **(**正解を表示します**)**

質問: **83**
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. Cisco Cloud Director
B. CiscoPrimeインフラストラクチャ
C. CDP AutoDiscovery
D. シードIP
E. PowerOn自動プロビジョニング
正解: **D,E (コメントを発表する)**

質問: **84**
クラウドでのデータ侵害を防ぐために使用される2つのパラメーターはどれですか？ 2つ選択してください。）
A. 複雑なクラウドベースのWebプロキシ
B. 暗号化
C. 強力なユーザー認証
D. DLPソリューション
E. なりすまし防止プログラム
正解: **(正解を表示します)**

質問: **85**
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: **86**
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: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.html 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.
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 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: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.html 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: 87
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. 精度
B. スケーラビリティ
C. セキュリティ
D. カプセル化
正解: (正解を表示します)

質問: 88

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: **89**
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. セキュリティカテゴリのブロック
B. コンテンツカテゴリのブロック
C. ファイル分析
D. アプリケーション制御
正解: **A (**コメントを発表する**)**

質問: **90**
認証後にセッションのAAA属性を変更するメカニズムを提供するRADIUS機能はどれですか。
A. CoA
B. 認証
C. 会計
D. 承認
正解: **(**正解を表示します**)**

質問: **91**
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. これらはシスコ独自のものです。
B. Pythonスクリプトをサポートしていません。
C. Cisco DNA Center API呼び出しを利用するには、Postmanが必要です。
D. ネットワークの全体的な状態を表示します
E. 新しいデバイスをすばやくプロビジョニングします。
正解: **(**正解を表示します**)**

質問: **92**
エンジニアがCiscoUmbrellaを設定しており、2つの異なるポリシーを参照するIDを持っています。.....使用が2番目の使用よりも優先されることを保証するアクションはどれですか？
A. ポリシーの順序で最初に正しいポリシーを作成します。
B. リクエストを正しいポリシーにリダイレクトするようにデフォルトのポリシーを構成します。
C. 最も具体的な構成のポリシーをポリシーの順序の最後に配置します。
D. 最後に変更されたタイムスタンプを持つポリシーのみを構成します。
正解: **(**正解を表示します**)**

質問: **93**
展示を参照してください。
エンジニアが証明書ベースのVPNを実装しています。既存の構成の結果は何ですか？
A. IKEv2ピア証明書のOUがMANGLERに設定されています
B. IKEv2ピア証明書のOUは、IKEv2認証ポリシーと一致するときにIDとして使用されます。
C. OU証明書属性がMANGLERに設定されているIKEv2ピアのみがIKEv2SAを正常に確立します
D. OUがMANGLERに設定されている場合、IKEv2ピア証明書のOUは暗号化されます
正解: **(**正解を表示します**)**

質問: **94**
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、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。
B. 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
C. 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
D. 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。
正解: **(**正解を表示します**)**

質問: **95**
最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

A. アクセスポリシーを変更します。
B. 識別プロファイルを変更します。
C. アウトバウンドマルウェアスキャンポリシーを変更する
D. Webプロキシ設定を変更する
正解**: A (**コメントを発表する**)**
URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow): - With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. - With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details. Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html
- With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic.
- With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details.
Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.
URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow): - With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. - With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details. Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html

質問: **96**
どのアルゴリズムが非対称暗号化を提供しますか？
A. AES
B. RSA
C. 3DES
D. RC4
正解: **B** (コメントを発表する)

質問: **97**
EPPソリューションはネットワークのどの部分にのみ焦点を当てており、EDRソリューションは焦点を当てていませんか？
A. コア
B. 東西ゲートウェイ
C. サーバーファーム
D. 周囲
正解: **D** (コメントを発表する)

質問: **98**
FlexVPNとDMVPNの違いは何ですか？
A. FlexVPNはIKEv2を使用し、DMVPNはIKEv1またはIKEv2を使用します
B. FlexVPNはIKEv1またはIKEv2を使用し、DMVPNはIKEv2のみを使用します
C. DMVPNはIKEv1のみを使用しますFlexVPNはIKEv2のみを使用します
D. DMVPNはIKEv1またはIKEv2を使用し、FlexVPNはIKEv1のみを使用します
正解: (正解を表示します)

質問: **99**
公開鍵と秘密鍵を使用する暗号化のタイプはどれですか？
A. 非線形
B. 非対称
C. 線形
D. 対称
正解: **B** (コメントを発表する)

質問: **100**
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: **(**正解を表示します**)**
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. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf 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.
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. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

質問: **101**
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 Duo
B. Cisco Umbrella
C. エンドポイント向けCisco AMP
D. Cisco AnyConnect
正解: **(**正解を表示します**)**

質問: **102**
展開内の他の管理対象デバイスと類似している可能性が高い管理対象デバイスの側面を定義する機能またはパラメーターの共有セットを表すポリシーはどれですか。
A. グループポリシー
B. アクセス制御ポリシー
C. デバイス管理ポリシー
D. プラットフォームサービスポリシー
正解: **(**正解を表示します**)**
Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings

policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.
administrative features.
A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.
For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.
Reference:
Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.

質問**: 103**
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. 保存されたCiscoASAファイアウォールの設定を取得します
B. グローバルルールをポリシーに追加します
C. CiscoASAのホスト名を変更します
D. ポリシーからグローバルルールを削除します
正解**: (**正解を表示します**)**

質問**: 104**

エンドポイントのセキュリティを確保するために、Cisco Identity Services Engineポスチャモジュールが提供する2つのアクションはどれですか (2つ選択してください)。
A. エンドポイントグループへの割り当ては、エンドポイント属性に基づいて動的に行われます。
B. エンドポイントサプリカント構成がデプロイされます。
C. 集中管理ソリューションが導入されています。
D. パッチ管理の修正を行います。
E. アクセスが許可される前に、最新のウイルス対策アップデートが適用されます。
正解: **(**正解を表示します**)**

質問: **105**
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: **A (**コメントを発表する**)**
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: **106**
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: **107**
ソフトウェア定義のネットワークアーキテクチャ内のコントローラーがネットワーク内のスイッチの構成を動的に変更する場合、どのタイプのAPIが使用されますか？
A. 西行きAP
B. サウスバウンドAPI
C. ノースバウンドAPI
D. イーストバウンドAPI
正解: **B (**コメントを発表する**)**
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.

質問: **108**
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ユーザーグループを指定します
B. SNMPUSMエントリを追加します
C. コミュニティ文字列を指定します。
D. SNMPマネージャーとUDPポートを指定します。
E. SNMPホストアクセスエントリを追加します
正解: **B,E (**コメントを発表する**)**

質問: **109**

管理者がネットワークに新しいスイッチを追加し、ネットワークアクセス制御用にAAAを設定しました。設定をテストするとき、RADIUSはCisco ISEに対して認証しますが、拒否されます。この設定にipradius source-interfaceコマンドが必要なのはなぜですか？
A. 暗号化されたRADIUS認証では、RADIUSソースインターフェイスを定義する必要があります
B. RADIUSソースインターフェイスが定義されている場合、RADIUS要求はルーターによってのみ生成されます。
C. RADIUS認証キーは、定義されたRADIUS送信元インターフェイスからのみ送信されます
D. 構成されたNASIPから発信された要求のみがRADIUSサーバーによって受け入れられます
正解: **C** (コメントを発表する)

質問: **110**
セキュリティイベントのみをログに記録するようにCiscoUmbrellaを構成するにはどうすればよいですか。
A. ポリシーごと
B. レポート設定で
C. [セキュリティ設定]セクション
D. [展開]セクションのネットワークごと
正解: (正解を表示します)
The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs. From the Policy wizard, log settings are: Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management From the Policy wizard, log settings are:
Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on.
The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs. From the Policy wizard, log settings are: Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

質問: **111**
説明を左側から右側の暗号化アルゴリズムにドラッグアンドドロップします。
正解:

質問: **112**
Firepower Next Generation Intrusion Prevention Systemで使用されている2つのアプリケーション層プリプロセッサはどれですか？ 2つ選択してください）
A. パケットデコーダー
B. SIP
C. modbus
D. インライン正規化
E. SSL
正解: **B,E (**コメントを発表する**)**
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.
application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.
Reference:
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

質問: **113**
セキュリティアプリケーションがソフトウェア定義のネットワークアーキテクチャ内のコントローラに特定のセキュリティの脅威について通知するときに使用されているAPIのタイプはどれですか？
A. サウスバウンドAPI
B. ノースバウンドAPI
C. イーストバウンドAPI
D. 西行きAP
正解: **A,B (**コメントを発表する**)**

質問: **114**
エンジニアがエンドポイント用にAMPを構成していて、特定のファイルの実行をブロックしたいと考えています。このタスクを実行するために使用されるアウトブレイク制御方法はどれですか？

A. アプリケーションブロックリスト
B. 簡単な検出
C. 高度なカスタム検出
D. デバイスフローの相関
正解: **(**正解を表示します**)**

質問: **115**
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。）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。
A. NTLMまたはKerberos認証レルムを作成し、透過的なユーザーID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. Cisco ContextDirectoryAgentなどの別のActiveDirectoryエージェントを展開します。
D. 別のeDirectoryサーバーを展開します :クライアントのIPアドレスはこのサーバーに記録されます
正解: **(**正解を表示します**)**

質問: **116**
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. 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
B. 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。
C. 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
D. 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
正解: **D (**コメントを発表する**)**

質問: **117**
展示を参照してください。
この出力を表示するために使用されたコマンドはどれですか？
A. dot1xをすべて表示
B. show dot1x interface gi1 / 0/12
C. dot1xを表示
D. dot1xのすべての概要を表示
正解: **(**正解を表示します**)**

質問: **118**
DMVPNとsVTIの違いは何ですか？
A. DMVPNは他のベンダーとの相互運用性を提供しますが、sVTIは提供しません。
B. DMVPNは動的トンネル確立をサポートしますが、sVTIはサポートしません。
C. DMVPNはトンネル暗号化をサポートしていますが、sVTIはサポートしていません。
D. DMVPNは静的トンネルの確立をサポートしますが、sVTIはサポートしません。

正解: **(**正解を表示します**)**

質問: **119**
WCCPでTCPトラフィックをリダイレクトするには、Cisco WSAでどのプロキシモードを使用する必要がありますか？
A. 透明
B. リダイレクト
C. フォワード
D. プロキシゲートウェイ
正解: **A (**コメントを発表する**)**
There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode. In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA.
There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode. In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf

質問: **120**
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: **121**
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、未知の高度な脅威について未知のサイトをテストしますか？
A. Cisco Identity Services Engine
B. Cisco Advanced Stealthwatch Appliance
C. CiscoWebセキュリティアプライアンス
D. Ciscoエンタープライズセキュリティアプライアンス
正解: **C** (コメントを発表する)

質問: **122**
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. システム追加<ホスト> <キー>を構成します
B. マネージャーの削除を構成する
C. configure manager add <host> <key>
D. マネージャーの構成<キー>ホストの追加
正解: **C** (コメントを発表する)

質問: **123**
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. 永遠の青い窓
B. ハートブリードSSLバグ
C. スペクターワーム
D. W32/AutoRunワーム
正解: (正解を表示します)

質問: **124**
ネットワークにCiscoESAを導入した後、一部のメッセージが宛先に到達できないことに気付きました。
各メッセージが失われた場所を特定するために、どのタスクを実行できますか？
A. メッセージ追跡を有効にするようにtrackingconfigコマンドを構成します。
B. システムレポートを生成します。
C. ログファイルを確認します。
D. トレースを実行します。
正解: **(**正解を表示します**)**
Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a spam quarantine - or if it is located somewhere else in the mail stream. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011110.html Reference:
Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a spam quarantine - or if it is located somewhere else in the mail stream. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011110.html

質問: **125**
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: **126**
展示を参照してください。
Cisco DNA Center APIのこのPythonスクリプトの結果は何ですか？
A. スイッチに関する情報を受信します
B. スイッチに認証を追加します
C. Cisco DNACenterにスイッチを追加します
正解: **C (**コメントを発表する**)**

質問: **127**
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. InfluxDB
C. Grafana
D. Splunk
正解: **(**正解を表示します**)**

質問: **128**
CiscoISE環境でのマイデバイスポータルの目的は何ですか。
A. 新しいラップトップとモバイルデバイスを登録する
B. 新しくプロビジョニングされたモバイルデバイスをリクエストする
C. ユーザーレスおよびエージェントレスシステムをプロビジョニングする
D. エンドユーザーが所有するシステムでウイルス対策の定義とパッチを管理および展開する
正解: **(**正解を表示します**)**
Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

質問: **129**
Cisco ISEサーバとADドメインを統合する際の前提条件は何ですか？
A. CiscoISEサーバとADサーバを同じサブネットに配置します
B. 共通の管理者アカウントを構成します
C. 共通DNSサーバーを構成する
D. CiscoISEサーバとADサーバのクロックを同期します
正解: **D (**コメントを発表する**)**
The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F
+ Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.
+ If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.
+ You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.
Reference:
The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

質問**: 130**
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**: 131**
展示を参照してください。
この構成では、15という数字は何を表していますか？
A. 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: **132**
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. ユーザーセッションの制限
B. Web使用制御
C. SOCKSプロキシサービス
D. 透過的なユーザーID
正解: **D (**コメントを発表する**)**

質問: **133**
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. 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。
B. ブリッジプロキシ展開として定義されます。
C. 透過プロキシ展開として定義されています。
D. 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。
E. 明示的なプロキシ展開として定義されています。
正解: **(**正解を表示します**)**

質問: **134**
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. 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
B. 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
C. 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
D. 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
E. 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
正解: **(**正解を表示します**)**

質問: **135**

Cisco ASAは、暗号化されたCisco UnifiedCommunicationsトラフィックのTLSプロキシをサポートする必要があります。Cisco UC Managerプラットフォームのどこに ASAを追加する必要がありますか？
A. 証明書の信頼リスト
B. エンタープライズプロキシサービス
C. エンドポイント信頼リスト
D. セキュリティで保護されたコラボレーションプロキシ
正解: **A** (コメントを発表する)

質問: **136**
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. 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
C. MPFが設定されていなくてもNSELイベントを生成します
D. アクティブスタンバイフェールオーバーペアのアクティブASAとスタンバイASAからNetFlowデータレコードを送信します
正解: (正解を表示します)

質問: **137**
DMVPNテクノロジーとFlexVPNテクノロジーの共通点は何ですか？
A. FlexVPNとDMVPNは、IS-ISルーティングプロトコルを使用してスポークと通信します
B. FlexVPNとDMVPNは新しいキー管理プロトコルを使用します
C. FlexVPNとDMVPNは同じハッシュアルゴリズムを使用します
D. IOSルーターはDMVPNとFlexVPNに対して同じNHRPコードを実行します
正解: **D** (コメントを発表する)
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. Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/ 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. Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/

質問: **138**
CiscoASAとゾーンベースのポリシーファイアウォールを備えたCiscoIOSルータの機能の違いは何ですか。
A. Cisco ASAはハイアベイラビリティ用に設定できますが、ゾーンベースのポリシーファイアウォールを備えたCiscoIOSルータは設定できません。
B. ゾーンベースのポリシーファイアウォールを備えたCisco IOSルータは、デフォルトですべてのトラフィックを拒否しますが、Cisco ASAは、ルールが追加されるまですべてのトラフィックを許可することから始めます。
C. Cisco ASAはデフォルトですべてのトラフィックを拒否しますが、ゾーンベースのポリシーファイアウォールを備えたCisco IOSルータは、信頼できないインターフェイスでもすべてのトラフィックを許可することから始めます。
D. ゾーンベースのポリシーファイアウォールを備えたCisco IOSルータは、ハイアベイラビリティ用に設定できますが、CiscoASAは設定できません。
正解: **(**正解を表示します**)**

質問: **139**
CiscoFirepowerのセキュリティインテリジェンスポリシーを使用して、Firepowerブロックベースの2つの基準はどれですか。
（2つ選択してください）
A. URL
B. プロトコルID
C. IPアドレス
D. MACアドレス
E. ポート番号
正解: **A,C (**コメントを発表する**)**
Security Intelligence Sources ... Custom Block lists or feeds (or objects or groups) Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.) For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/security_intelligence_blacklisting.html
...
Custom Block lists or feeds (or objects or groups)
Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.) For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy.
Security Intelligence Sources ... Custom Block lists or feeds (or objects or groups) Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.) For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed,

add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/security_intelligence_blacklisting.html

質問: **140**
説明を左側から右側の正しいプロトコルバージョンにドラッグアンドドロップします。
正解:

質問: **141**
パブリックコンピューティング環境に保存されている機密情報を特定することでデータ損失を削減するテクノロジーはどれですか？
A. Cisco SDA
B. Cisco Cloudlock
C. Cisco Firepower
D. Cisco HyperFlex
正解: **B (**コメントを発表する**)**

質問: **142**
展示を参照してください。
どのタイプの認証が使用されていますか？
A. MicrosoftOutlookのLDAP認証
B. POP3認証
C. SMTPリレーサーバー認証
D. 外部ユーザーとリレーメール認証
正解: **(**正解を表示します**)**
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.
messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
Reference:
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful

TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

質問: **143**
展示を参照してください。
組織は、ネットワーク内でDHCPスヌーピングを使用しています。新しいスイッチのVLAN41のユーザーが、IPアドレスが取得されていないと不満を言っています。ユーザーにネットワーク接続を提供するには、スイッチインターフェイスでどのコマンドを構成する必要がありますか？
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
正解: **(**正解を表示します**)**
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.
The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default.
In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

質問: **144**
Webセキュリティアプライアンスで透過認証が失敗した場合、エンドユーザーはどのタイプのアクセスを取得しますか？
A. ブロック
B. ゲスト
C. 限られたインターネット
D. フルインターネット

正解: **A** (コメントを発表する)

質問: **145**
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。この目標を達成するアクションはどれですか？
A. Cisco Umbrellaからのエラーを抑制するために、ユーザーのブラウザ設定を変更します。
B. 組織のルートCAをCiscoUmbrellaにアップロードします。
C. CiscoUmbrellaルートCAをユーザのデバイスにインストールします。
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: **146**
SQLインジェクション攻撃を軽減するために使用される2つの防止手法はどれですか？ 2つ選択してください。）
A. プリペアドステートメントとパラメーター化されたクエリを使用します。
B. オブジェクトリレーショナルマッピングライブラリを使用する代わりにSQLコードを記述します
C. ウェブとアプリ層の間の接続を保護します
D. Webアプリケーションデータベースログインで SQLコードの実行をブロックします。
E. 整数、浮動小数点数、またはブール値の文字列パラメータをチェックして、正確な値を確認します
正解: (正解を表示します)

質問: **147**
DNS層のセキュリティを活用してユーザーを保護するセキュリティソリューションはどれですか？
A. Cisco ISE
B. Cisco Umbrella
C. Cisco ASA
D. Cisco FTD
正解: **B** (コメントを発表する)

質問: **148**
エンジニアは、CiscoUmbrellを使用して特定のアドレスをブロックするようにポリシーを変更する必要があります。ポリシーはすでに作成されており、デフォルトのポリシー要素のu :としてアクティブになっています。このタスクを実行するには、他に何をする必要がありますか？
A. アプリケーション設定を変更して、アプリケーションのみが必要なアドレスに接続できるようにします。
B. コンテンツカテゴリを使用して、特定のアドレスをブロックまたは許可します。
C. 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。
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: (正解を表示します)

質問: **149**

Cisco Security Managerは何を管理していますか？
A. アクセスポイント
B. WSA
C. ASA
D. ESA
正解**: (**正解を表示します**)**
Cisco Security Manager provides a comprehensive management solution for: - Cisco ASA 5500 Series Adaptive Security Appliances - Cisco intrusion prevention systems 4200 and 4500 Series Sensors - Cisco AnyConnect Secure Mobility Client Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco intrusion prevention systems 4200 and 4500 Series Sensors
- Cisco AnyConnect Secure Mobility Client
Cisco Security Manager provides a comprehensive management solution for: - Cisco ASA 5500 Series Adaptive Security Appliances - Cisco intrusion prevention systems 4200 and 4500 Series Sensors - Cisco AnyConnect Secure Mobility Client Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html

質問**: 150**
NetFlowフローモニタリングの2つの機能は何ですか？ （2つ選択してください）
A. 入力および出力情報を追跡できます
B. フローレコードとフローインポーターを含める
C. すべての入力フロー情報をインターフェースにコピーします
D. インターフェースでのパケットサンプリングは必要ありません
E. マルチキャスト、MPLS、またはブリッジトラフィックの追跡に使用できます
正解**: (**正解を表示します**)**
The following are restrictions for Flexible NetFlow: + Traditional NetFlow (TNF) accounting is not supported. + Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported. + Both ingress and egress NetFlow accounting is supported. + Microflow policing feature shares the NetFlow hardware resource with FNF. + Only one flow monitor per interface and per direction is supported. Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html When configuring NetFlow, follow these guidelines and restrictions: + Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic. + NetFlow supports multicast IP traffic. Reference: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html
+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.
+ Both ingress and egress NetFlow accounting is supported.

+ Microflow policing feature shares the NetFlow hardware resource with FNF.
+ Only one flow monitor per interface and per direction is supported.
Reference:
consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html
When configuring NetFlow, follow these guidelines and restrictions:
+ Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic.
+ NetFlow supports multicast IP traffic.
The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN The following are restrictions for Flexible NetFlow: + Traditional NetFlow (TNF) accounting is not supported. + Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported. + Both ingress and egress NetFlow accounting is supported. + Microflow policing feature shares the NetFlow hardware resource with FNF. + Only one flow monitor per interface and per direction is supported. Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html When configuring NetFlow, follow these guidelines and restrictions: + Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic. + NetFlow supports multicast IP traffic. Reference: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html

質問**: 151**
管理者は、ユーザーが企業ネットワークへのアクセスを許可される前に、すべてのエンドポイントが準拠していることを確認したいと考えています。エンドポイントには、企業のウイルス対策アプリケーションがインストールされており、最新ビルドのWindowsが実行されている必要があります。
10.ネットワークで許可される前に、すべてのデバイスが準拠していることを確認するために、管理者は何を実装する必要がありますか？
A. CiscoStealthwatchとCiscoIdentity ServicesEngineの統合
B. Cisco Identity ServicesEngineおよびAnyConnectポスチャモジュール
C. PxGridサービスが有効になっているCisco Identity Services Engine
D. ダイナミックアクセスポリシーが設定されたCiscoASAファイアウォール
正解**: (**正解を表示します**)**

質問: **152**
エンドポイントレベルでソーシャルエンジニアリングやフィッシングと戦うのに役立つ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. Cisco DNA Center
B. Cisco Duo Security
C. Cisco TrustSec
D. Cisco Umbrella
E. Cisco ISE
正解: **B,D (**コメントを発表する**)**

質問: **153**
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. NIST
B. IETF
C. ANSI
D. IEEE
正解: **(**正解を表示します**)**

質問: **154**
右上の正しい定義に左から火力と次世代侵入防止システム検出器をドロップします。
正解:

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