Cisco.350-701J.v2021-07-08.q90

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：	90
バージョン：	v2021-07-08
ページの閲覧量：	442
問題集の閲覧量：	8364

https://www.jpnshiken.com/shiken/Cisco.350-701J.v2021-07-08.q90.html

質問: **1**

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

A. 複数のNetFlowコレクターがサポートされています。

B. 高度なNetFlowv9テンプレートとレガシーv5フォーマットがサポートされています。

C. フロー作成イベントが遅延します。

D. セキュアNetFlow接続はCisco PrimeInfrastructure用に最適化されています

正解: **A** (コメントを発表する)

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

質問: **2**

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

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

A. 暗号化係数

B. ナレッジファクター

C. 生体認証係数

D. 時間係数

E. 機密保持係数

正解: **B,C** (コメントを発表する)

質問: **3**

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す必要がある2つのサービスはどれですか。
2つ選択してください。）

A. スパム対策

B. ウイルス対策

C. 暗号化

D. DLP

E. DDoS

正解: **C,D** (コメントを発表する)

質問: **4**
Cisco Eメールセキュリティアプライアンスの主な役割は何ですか。
A. メール送信エージェント
B. メールユーザーエージェント
C. メール転送エージェント
D. メール配信エージェント
正解: (正解を表示します)

質問: **5**
AWSのCisco FTDvでサポートされている2つの導入モデル構成はどれですか？ （2つ選択してください。）
A. ルーテッドモードで構成され、オンプレミスの物理FMCアプライアンスによって管理されるCisco FTDv
B. 1つの管理インターフェイスと2つのトラフィックインターフェイスが構成されたCisco FTDv
C. 2つの管理インターフェイスと1つのトラフィックインターフェイスが構成されたCisco FTDv
D. ルーテッドモードで構成され、AWSにインストールされたFMCvによって管理されるCisco FTDv
E. ルーテッドモードで構成され、IPv6が構成されたCisco FTDv
正解: (正解を表示します)

質問: **6**
組織は、接続が確立される前に悪意のある宛先をブロックすることにより、多層防御を改善しようとしています。ソリューションは、特定のアプリケーションがネットワーク内で使用されるのをブロックできる必要があります。この目標を達成するには、どの製品を使用する必要がありますか？
A. Cisco Firepower
B. Cisco Umbrella
C. ISE
D. AMP
正解: (正解を表示します)

Cisco Umbrella uses the internet's infrastructure to block malicious destinations before a connection is ever established. Umbrella uses DNS to stop threats over all ports and protocols – even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

質問: **7**
Any-to-any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セキュアなVPN接続を実装するために使用する必要があるテクノロジー
A. IPsec DVTI
B. FlexVPN
C. DMVPN
D. VPNを取得
正解: (正解を表示します)

質問: **8**

展示を参照してください。

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

この出力を生成し、dot1xまたはmabで認証しているポートを表示するために使用されたコマンドはどれですか。

A. 認証セッションを表示

B. dot1xすべてを表示

C. 認証方法を表示

D. 認証登録を表示

正解: **(**正解を表示します**)**

質問: **9**

Cisco ASAは、暗号化されたCisco Unified Communications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。ASAをCisco UC Managerプラットフォームのどこに追加する必要がありますか？

A. エンドポイント信頼リスト

B. 安全なコラボレーションプロキシ

C. エンタープライズプロキシサービス

D. 証明書信頼リスト

正解: **(**正解を表示します**)**

質問: **10**

Context Directory Agentの機能は何ですか？

A. Active Directoryログを読み取り、IPアドレスをユーザー名にマッピングします

B. ユーザー識別のためにWebセキュリティアプライアンスに代わってユーザー認証要求を受け入れます

C. WebセキュリティアプライアンスからActive Directoryへのユーザー認証要求を中継します

D. ユーザーのグループメンバーシップを維持します

正解: **(**正解を表示します**)**

質問: **11**
組織は、CiscoUmbrellaを使用してURLブロッキングを実装しています。ユーザーは一部のサイトにアクセスできますが、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. インテリジェントプロキシとSSL復号化がポリシーで無効になっています。
D. 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。
正解: **(**正解を表示します**)**
https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-Intelligent-Proxy

質問: **12**
なぜユーザーはオンプレミスのESAとCESソリューションを選択するのですか？
A. サーバーチームはこのサービスを外部委託したいと考えています。
B. 機密データはオンサイトに残す必要があります。
C. ESAはインラインで展開されます。
D. 需要は予測できません。
正解: **(**正解を表示します**)**

質問: **13**
エンジニアがルーターに安全に接続しようとしていて、安全でないアルゴリズムが使用されないようにしたいと考えています。ただし、接続は失敗しています。この目標を達成するためにどのような行動を取るべきですか？
A. ip ssh port22コマンドを使用してポートを構成します。
B. ip sshserverコマンドを使用してSSHサーバーを有効にします。
C. no iptelnetコマンドを使用してtelnetを無効にします。
D. crypto key generatersaコマンドを使用してRSAキーを生成します。
正解: **(**正解を表示します**)**
https://learningnetwork.cisco.com/s/question/0D53i00000KsrhK/rsa-key

質問: **14**
ASAファイアウォール透過モードのブリッジグループの特徴は何ですか？」
A. 単一のアクセスルールでARPトラフィックを許可します。
B. これはレイヤー3セグメントであり、1つのポートとカスタマイズ可能なアクセスルールが含まれています。
C. 複数のインターフェースが含まれ、インターフェース間のアクセスルールはカスタマイズ可能です
D. BVIインターフェースにIPアドレスがあり、管理トラフィックに使用されます。
正解: **(**正解を表示します**)**
A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

質問: **15**

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. ノースバウンドAPI

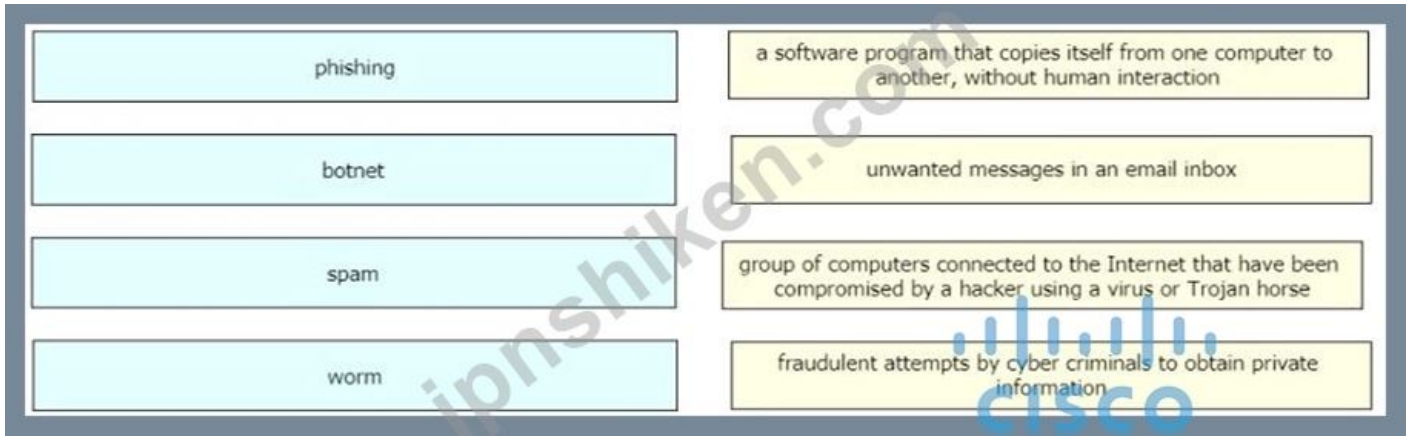
C. イーストバウンドAPI

D. サウスバウンドAPI

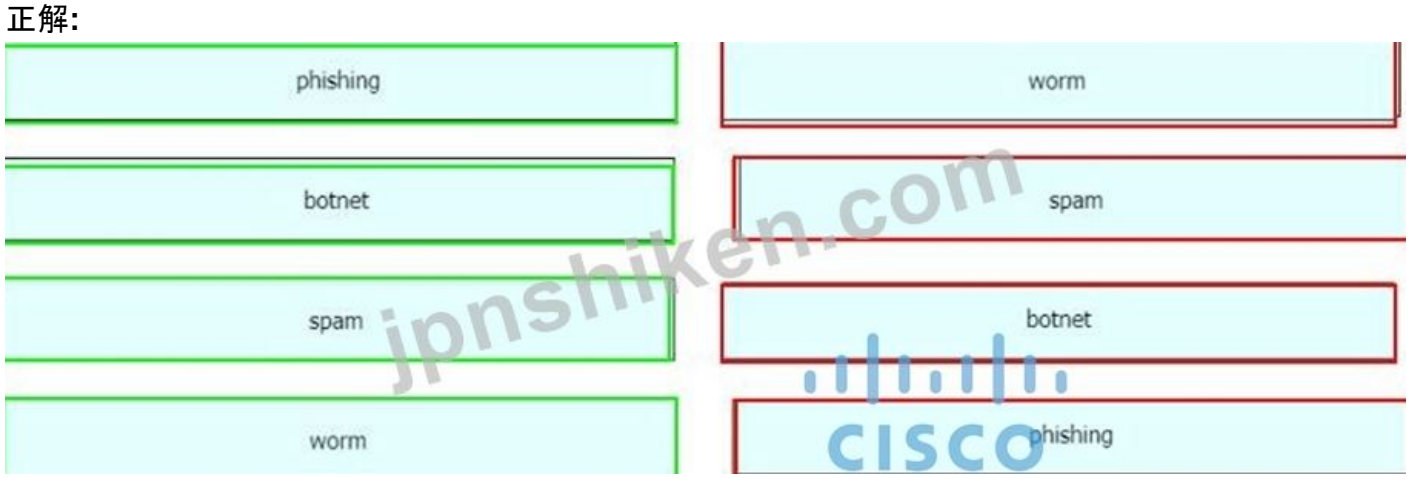
正解: **(**正解を表示します**)**

質問: **16**

一般的なセキュリティの脅威を左から右の定義にドラッグアンドドロップします。



正解:



質問: **17**

DMVPNテクノロジーとFlexVPNテクノロジーの共通点は何ですか？

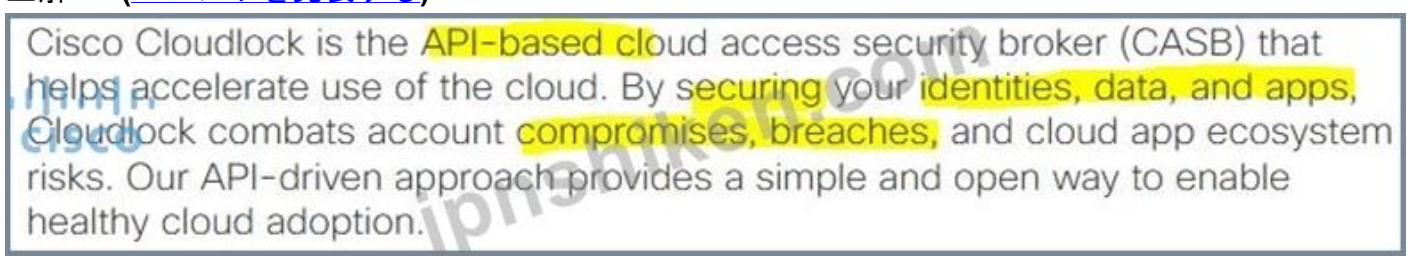
A. FlexVPNとDMVPNは同じハッシュアルゴリズムを使用します。

B. FlexVPNおよびDMVPNは新しいキー管理プロトコルを使用します。

C. FlexVPNおよび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

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)

質問: **18**
オンプレミスではない環境での侵害、アプリケーションリスク、およびデータ侵害を減らすのに役立つCisco APIベースのブローカーとは何ですか？
A. Cisco Cloudlock
B. Cisco Umbrella
C. Cisco AMP
D. Cisco App Dynamics
正解: **A** (コメントを発表する)



質問: **19**
Cisco DNA Center APIの2つの特徴は何ですか？　2つ選択してください）
A. ネットワークの全体的な状態を表示します
B. Pythonスクリプトをサポートしていません。
C. これらはシスコ独自のものです。
D. 新しいデバイスをすばやくプロビジョニングします。
E. Cisco DNA Center API呼び出しを利用するには、Postmanが必要です。
正解: (正解を表示します)

質問: **20**
ISEポスチャアセスメントを使用してエンドポイントをチェックできる2つの条件はどれですか？　2つ選択してください。）
A. コンピューターのID
B. ユーザーID
C. Windowsファイアウォール
D. Windowsサービス
E. デフォルトのブラウザー
正解: **C,D** (コメントを発表する)

質問: **21**
複数のセキュリティ製品間でデータを共有するには何を使用する必要がありますか？
A. Cisco Platform Exchange Grid
B. Cisco Advanced Malware Protection
C. Cisco Rapid Threat Containment

D. Cisco Stealthwatch Cloud
正解: **A** (コメントを発表する)

質問: **22**
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。
B. 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。
C. 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。
D. 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。
E. 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。
正解: (正解を表示します)

質問: **23**
Cisco Umbrellaのブラックリストに登録されるように指定されている個々のサイトはどこですか？
A. アプリケーション設定
B. 宛先リスト
C. セキュリティ設定
D. コンテンツカテゴリ
正解: **B** (コメントを発表する)

質問: **24**
ソーシャルエンジニアリングはどのタイプの攻撃ですか？
A. マルウェア
B. MITM
C. フィッシング
D. トロイの木馬
正解: (正解を表示します)

質問: **25**
ネットワーク上で現在何が発生しているのかを可視化して認識できるのは何ですか。
A. Telemetry
B. WMI
C. CMX
D. Prime Infrastructure
正解: (正解を表示します)

質問: **26**

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

質問: **27**
展示を参照してください。

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

エンジニアがネットワーク上で有線802.1xを構成しており、ラップトップを認証することができません。どのポート構成が欠落していますか？
A. dotlx再認証
B. dot1x paeオーセンティケーター
C. cisp enable
D. 認証オープン
正解: **(**正解を表示します**)**

質問: **28**
クロスサイトスクリプティングとSQLインジェクション、攻撃の違いは何ですか？
A. クロスサイトスクリプティングは企業の幹部が攻撃されるときですが、SQLインジェクションはデータベースが操作されるときです。
B. クロスサイトスクリプティングはリモートサイトを標的としたブルートフォース攻撃ですが、SQLインジェクションはソーシャルエンジニアリング攻撃です。
C. クロスサイトスクリプティングはサーバー側からコードが実行される攻撃ですが、SQLインジェクションはクライアント側からコードが実行される攻撃です。
D. クロスサイトスクリプティングは、コードがデータベースに挿入される攻撃ですが、SQLインジェクションは、コードがブラウザーに挿入される攻撃です。
正解: **(**正解を表示します**)**

質問: **29**
DNAC GUI以外の場所からネットワークをプログラムおよび監視する機能を提供するものは何ですか？
A. desktop client
B. ASDM
C. API
D. NetFlow

正解: **(**正解を表示します**)**

質問: **30**
組織にポリシーが設定されたCiscoESAがあり、違反に割り当てられたアクションをカスタマイズしたいと考えています。組織は、メッセージのコピーを配信し、メッセージを追加してDLP違反としてフラグを立てることを望んでいます。この機能を提供するには、どのアクションを実行する必要がありますか？
A. DLP違反でサブジェクトヘッダーを隔離および変更する
B. コピーを他の受信者に配信および送信する
C. 免責事項のテキストを配信して追加する
D. DLP違反通知を隔離して送信する
正解: **C (**コメントを発表する**)**

質問: **31**
crypto isakmp key ciscXXXXXXXX address 172.16.0.0コマンドを実行した結果はどうなりますか？
A. キーciscXXXXXXXXを使用して、IKE交換のすべての証明書を保護します
B. キーciscXXXXXXXXを使用して、172.16.0.0 / 16範囲のIKEv1ピアを認証します
C. キーciscXXXXXXXXを使用して172.16.0.0/32ピアのIPアドレスを認証します
D. キーciscXXXXXXXXを使用して、172.16.0.0 / 16範囲のIKEv2ピアを認証します
正解: **(**正解を表示します**)**

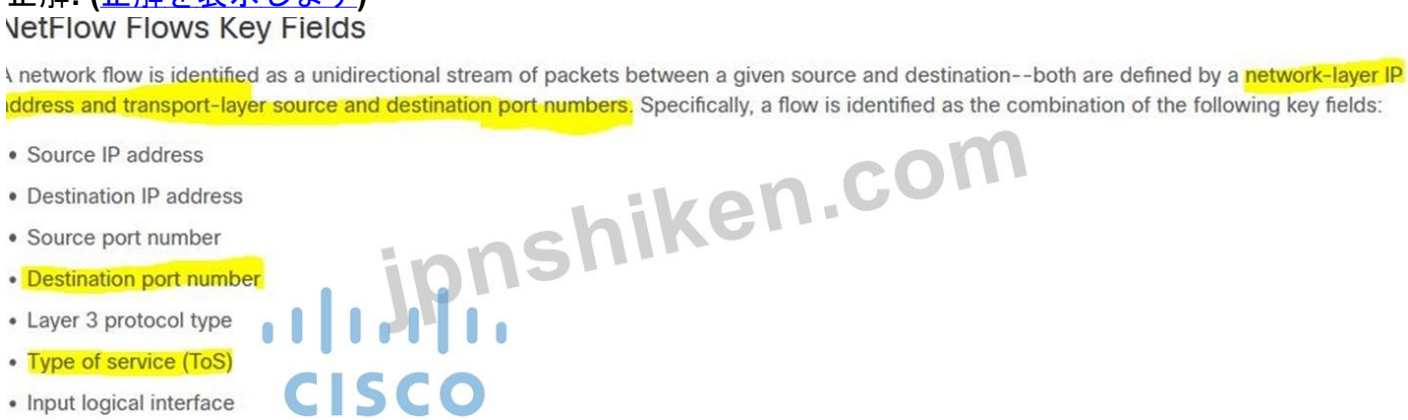
質問: **32**
組織には、Webアプリケーションをホストする2台のマシンがあります。マシン1はSQLインジェクションに対して脆弱ですが、マシン2はバッファオーバーフローに対して脆弱です。攻撃者がマシン1にアクセスできるが、マシン2にはアクセスできないようにするアクションは何ですか？
A. 2つのホスト間のパケットをスニッフィングする
B. 継続的なpingの送信
C. バッファのメモリがオーバーフローしています
D. 悪意のあるコマンドをデータベースに挿入する
正解: **(**正解を表示します**)**

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

質問: **33**
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. 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
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. 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
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
検出ルールを構成して、ホストおよびアプリケーションデータの検出をニーズに合わせて調整できます。
Firepowerシステムは、NetFlowエクスポーターからのデータを使用して、接続イベントと検出イベントを生成し、ホストとアプリケーションのデータをネットワークマップに追加できます。
ネットワーク分析ポリシーは、トラフィックがどのようにデコードおよび前処理されるかを管理するため、特に侵入の試みを示す可能性のある異常なトラフィックについて、さらに評価することができます。
正解: **(**正解を表示します**)**

質問: **34**
NetFlowフローで定義されている2つのフィールドはどれですか？ {2つ選択してください。）
A. サービスバイトのタイプ
B. レイヤー4プロトコルタイプ
C. サービスクラスビット
D. 出力論理インターフェース
E. 宛先ポート
正解: **(**正解を表示します**)**



質問: **35**
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. ネットワークディスカバリー
C. アクセス制御
D. パケットトレーサー
正解: **B (**コメントを発表する**)**

質問: **36**
展示を参照してください。

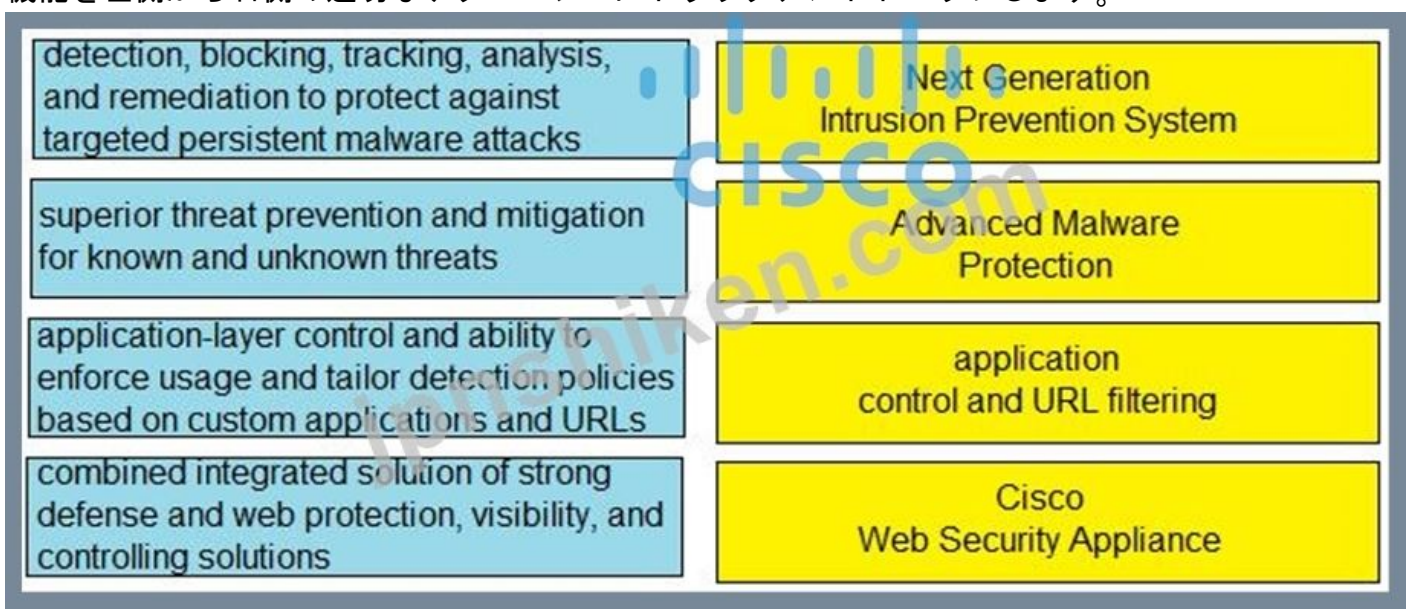
```
snmp-server group SNMP v3 auth access 15
```

この構成では、15という数字は何を表していますか？
A. SNMPv3認証試行間の秒単位の間隔
B. SNMPv3ユーザーがロックアウトされるまでに失敗する可能性のある試行の数
C. このルーターへの許可ユーザーの特権レベル
D. 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
正解: **(**正解を表示します**)**

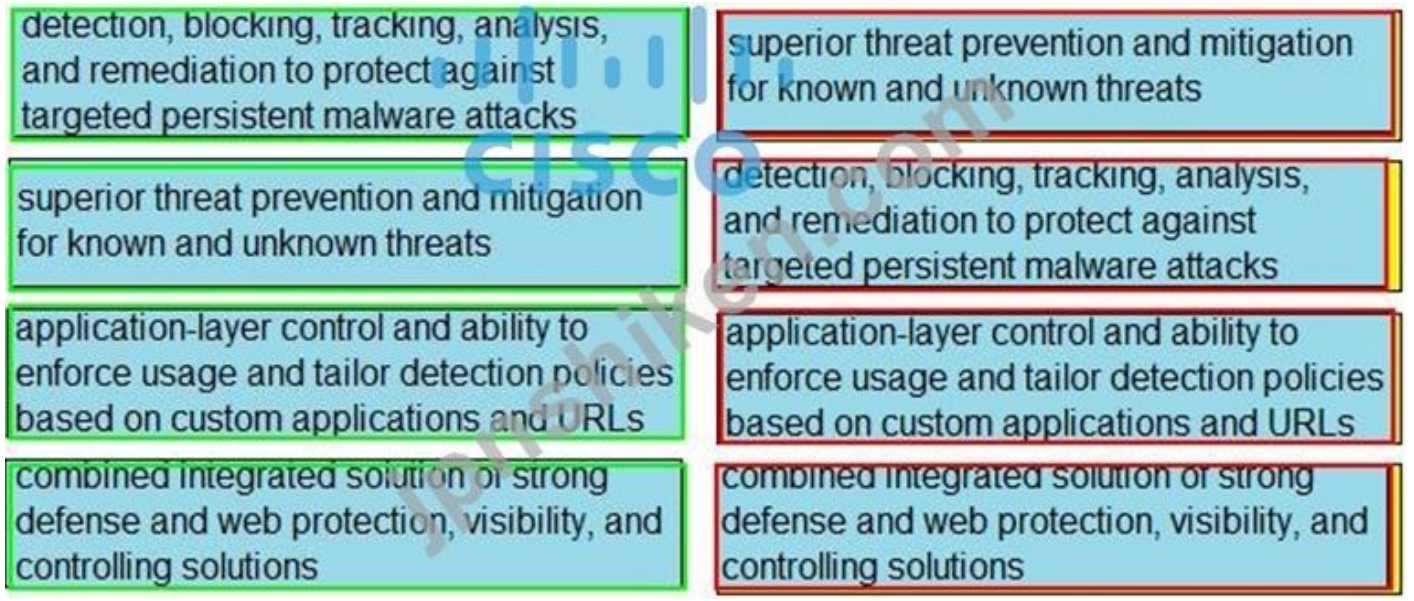
質問: **37**
WCCPでTCPトラフィックをリダイレクトするためにCisco WSAで使用する必要があるプロキシモードはどれですか。
A. transparent
B. forward
C. proxy gateway
D. redirection
正解: **(**正解を表示します**)**

質問: **38**
DevSecOpsはIT環境のどの部分に焦点を当てていますか？
A. アプリケーション開発
B. 境界ネットワーク
C. データセンター
D. ワイヤレスネットワーク
正解: **(**正解を表示します**)**

質問: **39**
機能を左側から右側の適切なテクノロジーにドラッグアンドドロップします。



正解:



質問: **40**

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

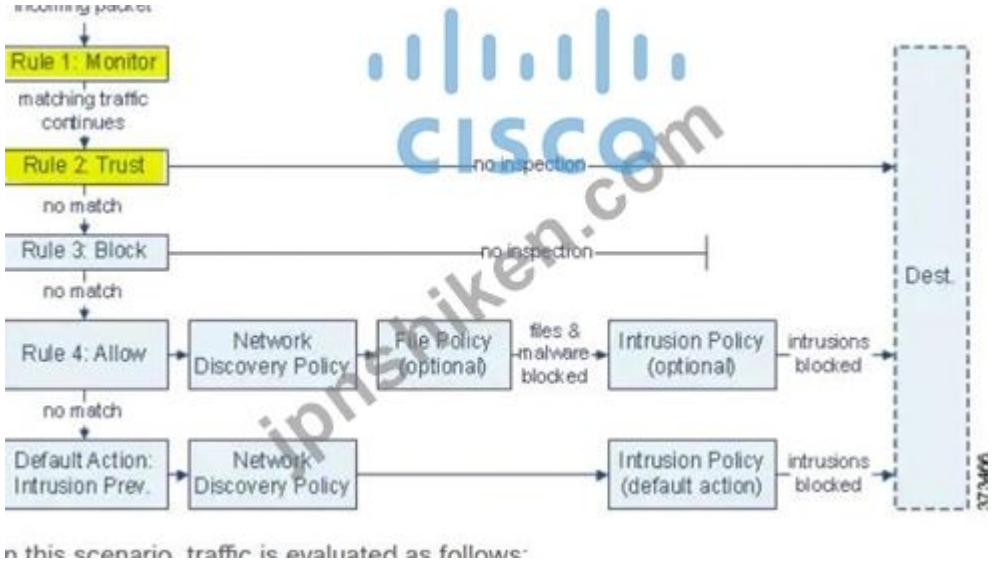
B. 信頼

C. リセット

D. 許可する

E. モニター

正解: **B,D** (コメントを発表する)



質問: **41**

モールは、共有アプライアンスを使用して顧客にセキュリティサービスを提供します。モールは、共有アプライアンスでの管理の分離を望んでいます。これらのニーズを満たすASA展開モードはどれですか。

A. マルチコンテキストモード

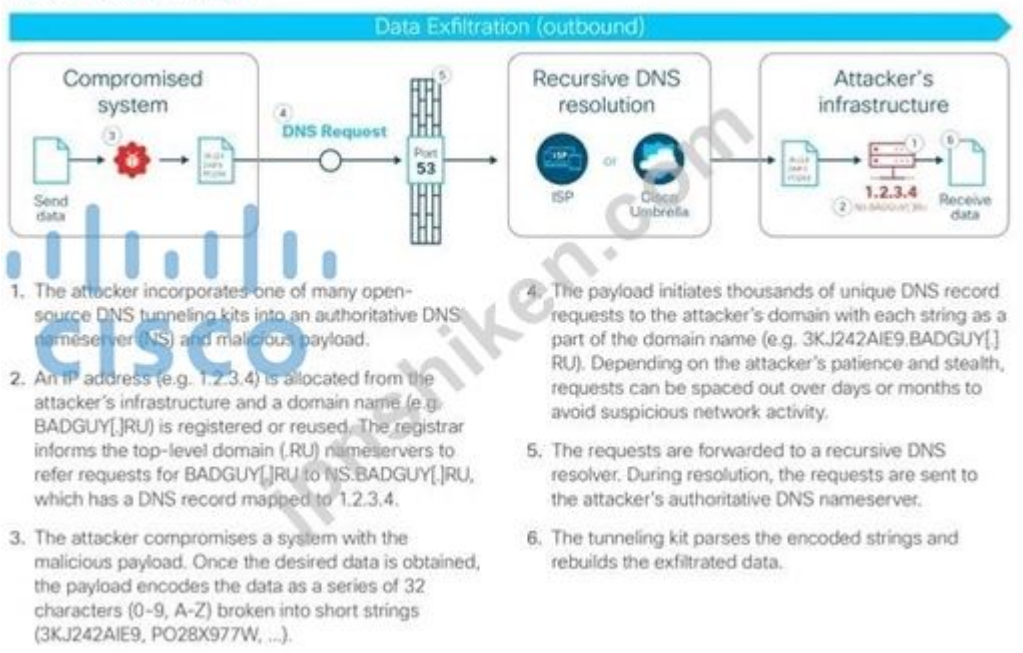
B. ルーテッドモード

C. 複数ゾーンモード

D. 透過モード
正解: **(**正解を表示します**)**

質問: **42**
DNSトンネリングはどのようにデータを盗み出しますか？
A. 攻撃者は、DNSレコードに基づいてクライアントが接続するドメインを登録し、その接続を介してマルウェアを送信します。
B. 攻撃者は逆引きDNSシェルを開いてクライアントのシステムに侵入し、マルウェアをインストールします。
C. 攻撃者は、非標準のDNSポートを使用して、組織のDNSサーバーにアクセスし、解決策を妨害します。
D. 攻撃者は、DNSリゾルバーが隠されているターゲットに電子メールを送信して、悪意のあるドメインにリダイレクトします。
正解: **(**正解を表示します**)**

Figure 1. **Data Exfiltration**



1. The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload.
2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. BADGUY[.]RU) is registered or reused. The registrar informs the top-level domain (.RU) nameservers to refer requests for BADGUY[.]RU to NS.BADGUY[.]RU, which has a DNS record mapped to 1.2.3.4.
3. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, PO28X977W, ...).
4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as a part of the domain name (e.g. 3KJ242AIE9.BADGUY[.]RU). Depending on the attacker's patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity.
5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker's authoritative DNS nameserver.
6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data.

質問: **43**
エンジニアは、Microsoft Windowsエンドポイントでポスチャチェックを使用し、MS17-010パッチがインストールされていないことを発見しました。これにより、エンドポイントはWannaCryランサムウェアに対して脆弱になります。この2つのソリューションは、このランサムウェア感染のリスクを軽減しますか？　2つ選択してください。）
A. Cisco Identity Services Engineでポスチャポリシーを設定して、ネットワークへのアクセスを許可する前に、エンドポイントのパッチレベルが満たされていることを確認します。
B. エンドポイントファイアウォールポリシーを設定して、エクスプロイトトラフィックがネットワーク全体で実行および複製されることを許可しないようにします。
C. 明確に定義されたエンドポイントパッチ戦略を設定して、エンドポイントに重大な脆弱性がタイムリーにパッチされるようにします。
D. Cisco Identity Service Engineでプロファイリングポリシーを設定して、ネットワークへのアクセスを許可する前に、エンドポイントのパッチレベルを確認します。
E. ネットワークへのアクセスを許可する前に、MS17-010パッチをインストールするようにCisco Identity Services Engineでポスチャポリシーを設定します。
正解: **A,E (**コメントを発表する**)**

質問: **44**
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. 管理コンソールとSDNコントローラー
B. SDNコントローラーとネットワーク要素
C. SDNコントローラーとクラウド
D. 管理コンソールとクラウド
正解: **(**正解を表示します**)**

質問: **45**
アプリケーションの可視性とセグメンテーションでハイブリッドクラウド展開ワークロードを保護するソリューションはどれですか。
A. Firepower
B. Nexus
C. Tetration
D. Stealthwatch
正解: **(**正解を表示します**)**

質問: **46**
AESに有効な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ビットブロックサイズ、168ビットキー長
B. 192ビットのブロックサイズ、256ビットのキー長
C. 128ビットブロックサイズ、256ビットキー長
D. 64ビットブロックサイズ、112ビットキー長
E. 128ビットブロックサイズ、192ビットキー長
正解: **(**正解を表示します**)**

質問: **47**
管理者ログインを機能させるために、Cisco ISEでシャドウユーザーを作成する必要があるIDストアはどれですか。
A. LDAP
B. 内部データベース
C. RSA SecureID
D. Active Directory
正解: **(**正解を表示します**)**

質問: **48**

Cisco Stealthwatch Cloudはクラウド環境にセキュリティをどのように提供しますか？
A. インターネットベースのDNS保護をクライアントとサーバーに割り当てます。
B. パブリックネットワークとプライベートネットワーク間の安全な接続を促進します。
C. デリケートなdatAの流出を防ぎます。
D. 可視性と脅威の検出を提供します。
正解: **D** (コメントを発表する)

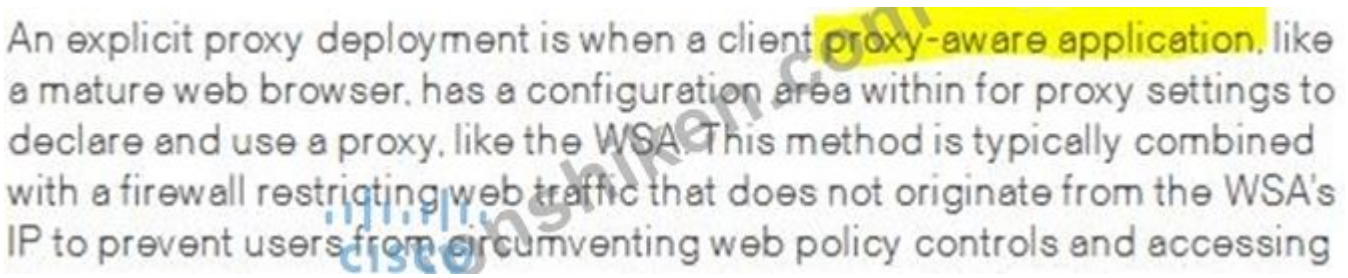
質問: **49**
展示を参照してください。

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

ネットワーク管理者がadmm5ユーザーのコマンド許可を構成します。この構成後、admin5ユーザーはHQ_Routerで何ができますか？
A. インターフェイスのIPアドレスを設定します
B. サブインターフェースを追加
C. 構成なしで完了
D. すべての構成を完了します
正解: (正解を表示します)

質問: **50**
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. SHA-384
B. AES-GCM
C. AES-256
D. SHA-96
正解: **B** (コメントを発表する)

質問: **51**
最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？
A. アクセスポリシーを変更します。
B. 識別プロファイルを変更します。
C. アウトバウンドマルウェアスキャンポリシーを変更する
D. Webプロキシ設定を変更する
正解: (正解を表示します)



質問: **52**
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. ティアドロップ
B. 土地
C. MITM
D. スマーフ
正解: **(**正解を表示します**)**

質問: **53**
Cognitive Threat Analyticsの2つの検出および分析エンジンとは何ですか？　2つ選択してください。）
A. インテリジェントプロキシ
B. データの引き出し
C. URLの分類
D. コマンドおよび制御通信
E. snort
正解: **(**正解を表示します**)**

質問: **54**
ユーザーがセキュリティの脅威を見つけるように訓練されており、ネットワークデバイスがすでに脅威の防止に役立っているにもかかわらず、エンドポイントに論理的なセキュリティ制御を設定することが重要なのはなぜですか？
A. 多層防御がネットワークで停止するため
B. エンドポイントの盗難を防ぐため
C. ヒューマンエラーまたは内部脅威が依然として存在するため
D. エンドポイントをより多くの脅威にさらす
正解: **(**正解を表示します**)**

質問: **55**
エンドポイント用の十分に確立されたパッチソリューションがない場合、会社はどの2つのリスクに脆弱ですか？　2つ選択してください。）
A. exploits
B. malware
C. ARP spoofing
D. denial-of-service attacks
E. eavesdropping
正解: **A,B (**コメントを発表する**)**

質問: **56**
エンジニアがCisco ESAを設定していて、受信者アドレスへの電子メールメッセージを受け入れるか拒否するかを制御したいと考えています。許可された受信者アドレスが含まれているリストはどれですか？
A. HAT
B. BAT
C. RAT
D. SAT
正解: **(**正解を表示します**)**

質問: **57**
攻撃者は、ターゲットシステムにアクセスできるように、ターゲットシステムで偵察を実行する必要があります。システムのパスワードが弱く、VPNリンクが暗号化されておらず、システムのアプリケーションにソフトウェアのバグがあります。攻撃者がパスワードがクリアテキストで送信されていることを確認できる脆弱性はどれですか？
A. 認証用の弱いパスワード
B. 不適切なファイルセキュリティ
C. アプリケーションのソフトウェアバグ
D. トラフィックの暗号化されていないリンク
正解: **(**正解を表示します**)**
https://www.cisco.com/ELearning/bulk/public/celc/CRS/media/targets/resources_mod07/7_3_5_improving_security.pdf

質問: **58**
Cisco Firepower Next Generation Intrusion Prevention Systemでネットワークディスカバリポリシーが必要な機能はどれですか。
A. セキュリティインテリジェンス
B. 影響フラグ
C. ヘルスモニタリング
D. URLフィルタリング
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/introduction_to_network_discovery_and_identity.html?bookSearch=true

質問: **59**
Cisco ESA管理者は、隔離された電子メールが配信される前にウイルスがないことを確認するようにCiscoESAを設定する必要があります。さらに、既知の不良メールサーバーからのメールの配信を防止する必要があります。これらの要件を満たすために実行する必要がある2つのアクションはどれですか？　2つ選択してください）
A. SenderBaseのアウトブレイクフィルターを使用する
B. メッセージ追跡サービスを有効にする
C. 受信者アクセステーブルを設定します
D. CiscoESAをDMZに導入します
E. アンチウイルス署名を使用して隔離された電子メールをスキャンします。

正解: **(**正解を表示します**)**
We should scan emails using AntiVirus signatures to make sure there are no viruses attached in emails.
Note: A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus.
SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers. When the Cisco ESA receives messages from known or highly reputable senders, it delivers them directly to the end user without any content scanning. However, when the Cisco ESA receives email messages from unknown or less reputable senders, it performs antispam and antivirus scanning.
Reference:
/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html

質問: **60**
Cisco Firepower Next Generation Intrusion Prevention Systemのホスト情報をキャプチャするためにどのポリシーが使用されますか？
A. 侵入
B. アクセス制御
C. ネットワーク検出
D. 相関
正解: **(**正解を表示します**)**

質問: **61**
インターネットブラウザを使用してクラウドベースのサービスにアクセスすると、どのようなリスクが発生しますか？
A. APIの安全でない実装
B. クラウドコネクタへの断続的な接続
C. 不正アクセスを許可するインフラの設定ミス
D. プロトコル内の脆弱性
正解: **A (**コメントを発表する**)**

質問: **62**
展示を参照してください。

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C         1.1.1.0 255.255.255.0 is directly connect, outside
S         172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C         192.168.100.0 255.255.255.0 is directly connected, inside
C         172.16.10.0 255.255.255.0 is directly connected, dmz
S           10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz
```

```
access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```

構成の結果は何ですか？

A. 内部ネットワークからのトラフィックがリダイレクトされます。
B. DMZネットワークからのトラフィックがリダイレクトされます。
C. 内部およびDMZネットワークからのトラフィックがリダイレクトされます。
D. すべてのTCPトラフィックがリダイレクトされます。
正解: **(**正解を表示します**)**

質問: **63**
CiscoISE環境でのマイデバイスポータルの目的は何ですか。
A. エンドユーザーが所有するシステムでウイルス対策の定義とパッチを管理および展開する
B. 新しいラップトップとモバイルデバイスを登録する
C. ユーザーレスおよびエージェントレスシステムをプロビジョニングする
D. 新しくプロビジョニングされたモバイルデバイスをリクエストする
正解: **(**正解を表示します**)**

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

質問: **64**
どのタイプのアルゴリズムがブルートフォース攻撃に対して最高レベルの保護を提供しますか？
A. HMAC
B. MD5
C. SHA
D. PFS

正解: **(**正解を表示します**)**

質問: **65**

展示を参照してください。

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

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


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

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

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

A. Firepower ThreatDefenseアプライアンスでスプリットトンネルポリシーが定義されていません。

B. サイト間VPNピアは異なる暗号化アルゴリズムを使用しています。

C. アクセス制御ポリシーはでVPNトラフィックを許可していません。

D. サイト間VPN事前共有キーが一致していません。

正解: **A (**コメントを発表する**)**

質問: **66**

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ているアウトブレイクコントロール方法はどれですか。

A. デバイスフロー相関

B. 単純な検出

C. 高度なカスタム検出

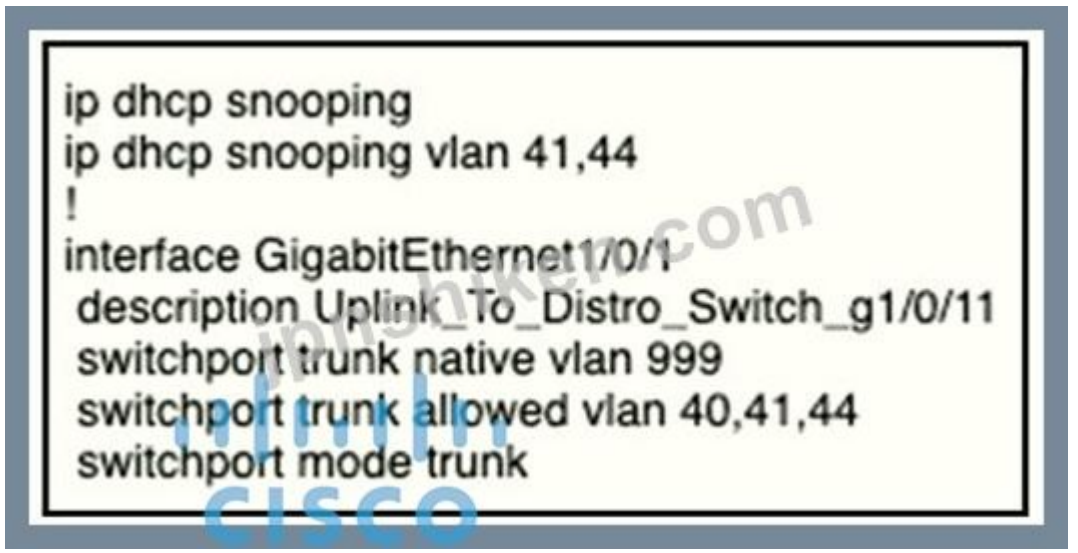
D. アプリケーションブロッキングリスト
正解: **(**正解を表示します**)**

質問: **67**
ゲストサービスのISEを認証するためにユーザーをWebポータルにリダイレクトするために使用されるメカニズムはどれですか。
（2つ選択してください。）
A. TACACS +
B. シングルサインオン
C. 多要素認証
D. 中央Web認証
E. ローカルWeb認証
正解: **D,E (**コメントを発表する**)**

質問: **68**
2つのDDoS攻撃カテゴリとは何ですか？ （2つ選択してください。）
A. ソースベース
B. ボリュームベース
C. データベース
D. シーケンシャル
E. プロトコル
正解: **(**正解を表示します**)**

質問: **69**
組織は最近CiscoWSAをインストールし、AVCエンジンを利用して、組織がアプリケーション固有のアクティビティを制御するポリシーを作成できるようにしたいと考えています。AVCエンジンを有効にした後、これを実装するには何をする必要がありますか？
A. セキュリティサービスを使用して、トラフィックモニターを構成します。
B. URL分類を使用して、アプリケーショントラフィックを防止します。
C. アクセスポリシーグループを使用して、アプリケーション制御設定を構成します。
D. Webセキュリティレポートを使用してエンジン機能を検証する
正解: **C (**コメントを発表する**)**
Explanation
The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

質問: **70**
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**)**

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html

質問: **71**

ICMPはどのようにして流出技術を使用しますか？

A. 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と制御タスクを実行する
B. 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ソースIPアドレスを含む多数のICMPパケットを送信する
C. ICMPエコー要求パケットでターゲットホストを圧倒する
D. 到達不能なパケットで宛先ホストをあふれさせる

正解: **A (**コメントを発表する**)**

質問: **72**

展示を参照してください。

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

response_json = response.json()

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


Ciscoセキュリティアプライアンスに接続されている場合、APIは何をしますか？
A. ネットワーク内のコンピューターからプロセスとPID情報を取得します
B. AMPが認識しているコンピューターに関するネットワークインターフェイス情報を収集する
C. エンドポイントのAMPからネットワークテレメトリ情報を収集します
D. AMPを管理するためのSNMPプルメカニズムを作成する
正解: **(**正解を表示します**)**

質問: **73**
IPsecで使用される2つの暗号化アルゴリズムはどれですか？ {2つ選択してください。）
A. AES-BAC
B. AES-ABC
C. HMAC-SHA1 / SHA2
D. トリプルAMC-CBC
E. AES-CBC
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book/sec-cfg-vpn-ipsec.html

質問: **74**
エンジニアは、特定のOU1を持つエンドポイントを新しいエンドポイントグループに自動的に割り当てたいと考えています。

このタイプのプロファイリングを機能させるには、どのプローブを有効にする必要がありますか？
A. DHCP
B. NMAP
C. SNMP
D. NetFlow
正解: **(**正解を表示します**)**

質問: **75**
Cisco DNA Centerを使用して実行できる2つのアクティビティはどれですか。 （2つ選択してください。）
A. プロビジョニング
B. 会計
C. デザイン
D. DNS
E. DHCP
正解: **(**正解を表示します**)**

質問: **76**
可能な限り強力なセキュリティをサポートするには、どのSNMPv3構成を使用する必要がありますか？
A. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
正解: **(**正解を表示します**)**

質問: **77**
マネージドIntercloudFabricデプロイメントモデルの2つのタイプは何ですか？　（2つ選択してください。）

A. パブリックマネージド
B. サービスプロバイダーが管理
C. エンタープライズ管理
D. ユーザー管理
E. ハイブリッドマネージド
正解: **(**正解を表示します**)**

質問: **78**
エンジニアは、ホスト上の悪意のあるアクティビティを検出するために行動分析を必要とし、クラウドプロバイダーのメカニズムを使用してテレメトリをセキュリティデバイスに送信するように組織のパブリッククラウドを構成しています。
この目標を達成するために、エンジニアはどのメカニズムを構成する必要がありますか？
A. ミラーポート
B. NetFlow
C. フロー
D. VPCフローログ
正解: **D (**コメントを発表する**)**
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/q-and-a-c67-737402.html

質問: **79**
Cisco IOS PKIの場合、CRLの配布ポイントとして使用される2種類のサーバはどれですか。
A. SCP
B. LDAP
C. 下位CA
D. SDP
E. HTTP
正解: **(**正解を表示します**)**

質問: **80**
ネットワーク管理者は、アクセス制御ポリシーで特定のURLをブロックするルールを構成し、
「チャットとインスタントメッセージング」カテゴリ。この目標を達成するには、どのレピュテーションスコアを選択する必要がありますか？
A. 1
B. 10
C. 5
D. 3
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/esa/esa111/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01111.html

質問: **81**
2つのDDoS攻撃カテゴリとは何ですか？ （2つ選択してください。）
A. シーケンシャル
B. プロトコル
C. データベース
D. ボリュームベース
E. スクリーベース
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

質問: **82**
組織が既知の悪意のあるドメインからスパムメールを受信している最初のTCP通信中にセッションを防ぐために何を構成する必要がありますか？
A. 悪意のある電子メールをドロップするようにCiscoESAを設定します。
B. 悪意のある電子メールを隔離するようにポリシーを構成します。
C. 通信を停止および拒否するようにポリシーを構成します
D. TCP接続をリセットするようにCiscoESAを設定します。
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118219-configure-esa-00.html

質問: **83**
ネットワーク管理者は、802.1X用のCiscoISEを使用するようにスイッチを設定しています。エンドポイントが認証に失敗しており、ネットワークにアクセスできません。管理者は、認証の詳細を確認するためにどこからトラブルシューティングを開始する必要がありますか？
A. コンテキストの可視性
B. 適応型ネットワーク制御ポリシーリスト
C. 会計レポート
D. RADIUSライブログ
ISEで失敗した認証と許可をトラブルシューティングする方法
ISEライブログを確認してください
プライマリISEポリシー管理ノード（PAN）にログインします。
[操作]> [RADIUS]> [ライブログ]に移動します
（オプション）イベントがRADIUSライブログに存在しない場合は、[操作]> [レポート]> [レポート]> [エンドポイントとユーザー]> [RADIUS認証]に移動し、ログで失敗した認証試行を確認します。
正解: **(**正解を表示します**)**

質問: **84**
設定されたポスチャポリシー要件が満たされていない場合、どのコンプライアンスステータスが表示されますか？
A. 準拠
B. 不明

C. 非準拠
D. 承認済み
正解: **(**正解を表示します**)**

質問: **85**
クラウド導入へのリスクを検討する場合、どの展開モデルが最も安全ですか？
A. パブリッククラウド
B. ハイブリッドクラウド
C. コミュニティクラウド
D. プライベートクラウド
正解: **D (**コメントを発表する**)**

質問: **86**
フィッシング攻撃を制御するために使用されているメカニズムはどれですか？ 2つ選択してください。）
A. 期限切れのWebサイトのCRLを取り消します。
B. 不正なWebサイトのブラウザーアラートを有効にします。
C. セキュリティグループメンバーシップを定義します。
D. スパイウェア対策ソフトウェアを使用します。
E. メールフィルタリングテクニックを実装します。
正解: **B,E (**コメントを発表する**)**

質問: **87**
プロキシキャッシングによってWebトラフィックのパフォーマンスを向上させるために使用されているテクノロジーはどれですか。
A. FireSIGHT
B. 火力
C. ASA
D. WSA
正解: **(**正解を表示します**)**

質問: **88**
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: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/security/esa/esa120/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01100.html

質問: **89**
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: **(**正解を表示します**)**
Explanation
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:
/m_ise_devices_byod.html

質問: **90**
Flexible NetFlowレコードの2つの利点は何ですか？　2つ選択してください）
A. ユーザーがフロー情報を構成してカスタマイズされたトラフィック識別を実行できるようにします
B. アカウンティングと請求の機能強化を提供します
C. レイヤー2から4までの幅広いIPパケット情報の監視を提供します。
D. 複数の会計テクノロジーを1つの会計メカニズムに統合します
E. トラフィックをドロップすることで攻撃を防止します。
正解: **(**正解を表示します**)**