CompTIA.CNX-001.v2025-07-28.q58

試験コード:	CNX-001
試験名称:	CompTIA CloudNetX Certification Exam
認定資格:	CompTIA
無料問題数:	58
バージョン:	v2025-07-28
アクセス数:	547
ページビュー数:	580
https://www.jpnpdf.com/CompTIA.CNX-001.v2025-07-28.q58-mondaishu.html	

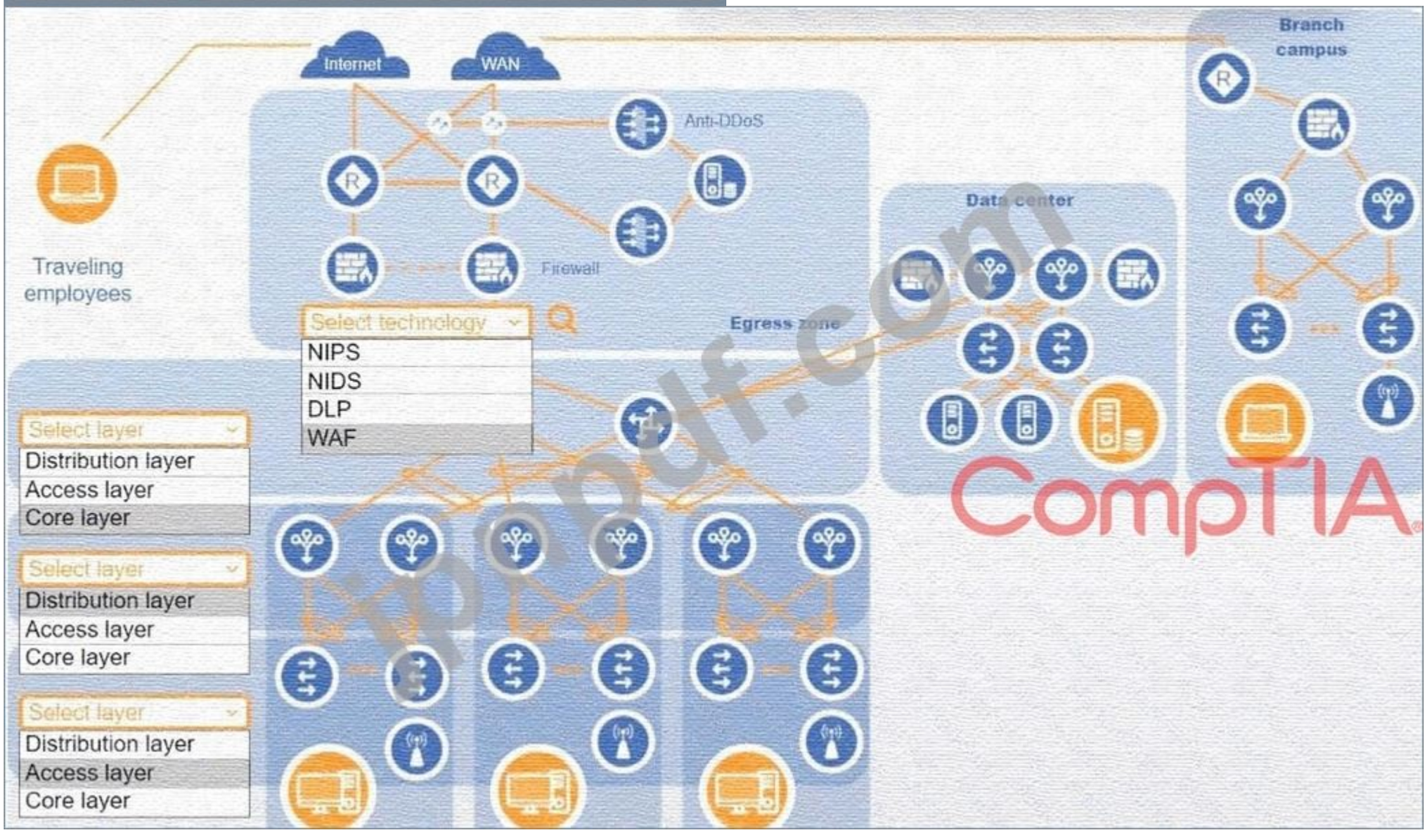
最新問題: **1**
ある企業は、ネットワークに関する数多くの問題を抱えており、サポートチームの拡大を決定しました。新入社員は、できる限り短期間で業務に慣れ、最小限のサポートで問題を解決できるようにする必要があります。この目標を達成するために、企業は以下のどれを構築すべきでしょうか？
A. トラブルシューティング時に各若手社員が行うべきことを文書化した作業指示書
B. ネットワークの問題とナレッジベースの記事について明確に文書化されたランブック
C. ネットワークインフラストラクチャ全体の物理および論理ネットワーク図
D. 各若手社員がネットワークインフラストラクチャに慣れるまで指導するメンタープログラム
Answer: (解答を表示する)
正確な抜粋からの包括的かつ詳細な説明：
ランブックとナレッジベースの記事には、よくある問題を解決するための手順が段階的に記載されており、新入社員が最小限の監督で迅速に生産性を向上できるよう支援します。これらのドキュメントは、新たな問題が発生するたびに更新でき、基礎的なトレーニングおよび運用リソースとして役立ちます。
CompTIA CloudNetX CNX-001 学習ガイドの 「運用ドキュメントと知識移転」の関連抜粋:
「ランブックには、定期的な運用タスクを処理するための標準化された手順が含まれています。ナレッジベースの記事を活用することで、最小限の監視で一貫したトラブルシューティングと解決が可能になります。」その他のオプション：
* A. 作業明細書 (SOW) は、トレーニングではなく、プロジェクトの成果物を定義するために使用されます。
* C. ネットワーク図はアーキテクチャを理解するのに役立ちますが、運用手順を理解するのには役立ちません。
* D. メンター プログラムは役立ちますが、拡張性がなく、すぐにトラブルシューティング手順を提供することはできません。

最新問題: **2**
ある企業がすべてのサービスをクラウドに移行した後、セキュリティ監査担当者は、多くのユーザーがさまざまなサービスで管理者ロールを付与されていることを発見しました。この企業は、次のようなソリューションを必要としていました。
クラウド上のサービスを保護します。
管理ロールへのアクセスを制限します。
限られた時間内に重要なサービスに対する管理ロールのリクエストを承認するためのポリシーを作成します。
管理者ロールのパスワードのローテーションを強制します。
管理ロールの使用状況を監査します。

会社の要件を満たす最善の方法は次のどれですか?
A. 特権アクセス管理
B. セッションベースのトークン
C. 条件付きアクセス
D. アクセス制御リスト
Answer: A (メーッセージを残す**)**
特権アクセス管理 (PAM) ソリューションは、管理ロールへのジャストインタイムの昇格を提供し、時間制限付きアクセスによる承認ワークフローを強制し、資格情報のローテーションを要求し、すべての特権セッションの包括的な監査を提供し、企業の要件を完全に満たします。

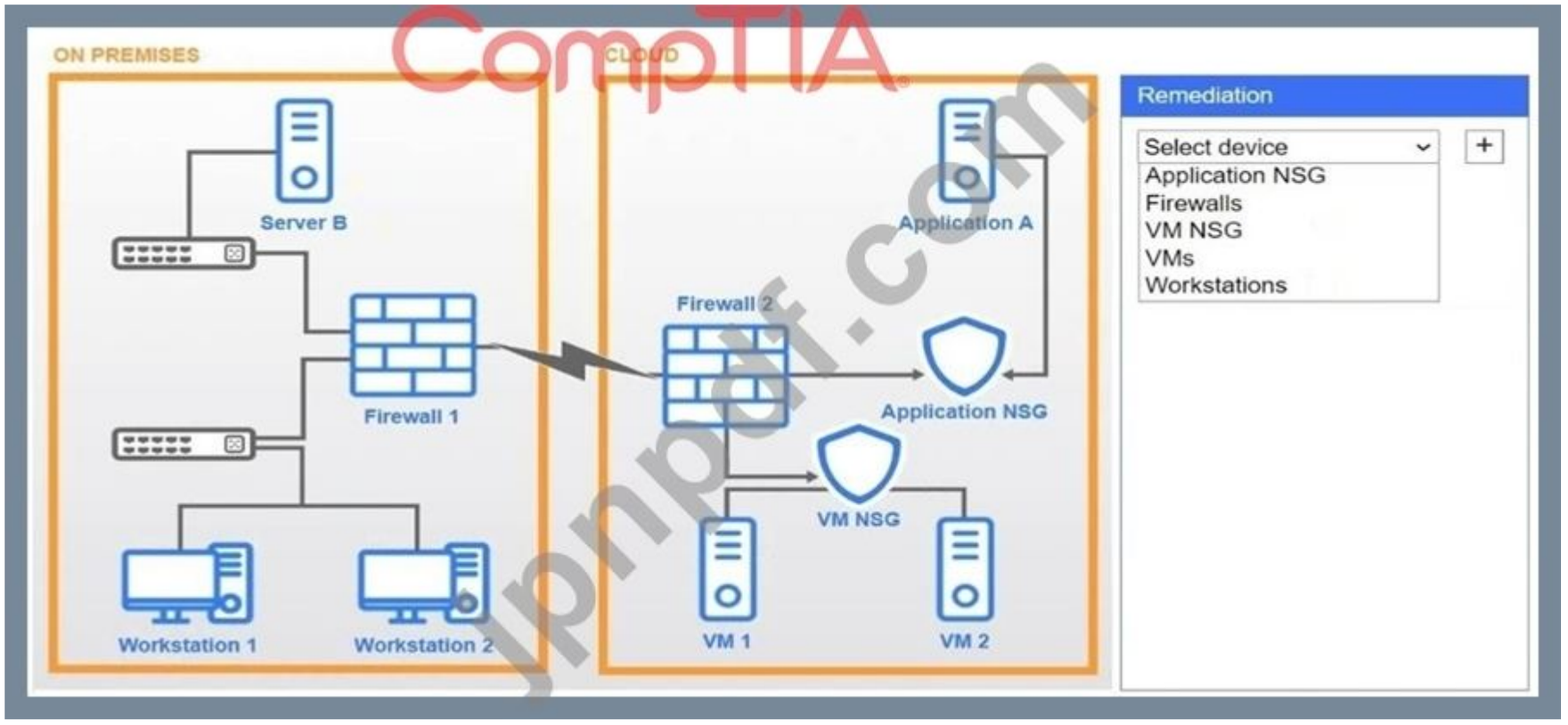
最新問題**: 3**
3 層階層のキャンパス ネットワークを設計しており、拠点と出張中の従業員間の安全な接続を確保する必要があります。
説明書
ネットワーク上のサーバー、ラップトップ、ワークステーションをクリックして、コマンド出力を確認します。
ドロップダウン メニューを使用して、図の各レイヤーに適切なテクノロジとラベルを決定します。
オプションは 1 回だけ使用できます。
追加の構成変更を行うには、虫眼鏡をクリックします。
いつでもシミュレーションの初期状態に戻したい場合は、 すべてリセット」ボタンをクリックしてください。

Answer:



最新問題: 4

ネットワーク管理者は、ハイブリッドクラウド環境における接続の問題を解決する必要があります。ワークステーションとVMはアプリケーションAにアクセスできません。ワークステーションはサーバーBにアクセスできます。
説明書
ワークステーション、VM、ファイアウォール、NSG をクリックしてトラブルシューティングを行い、情報を収集します。ターミナルに「help」と入力すると、使用可能なコマンドの一覧が表示されます。
修復が必要な適切なデバイスを選択し、関連する問題を特定します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



Remediation

Select device

- Application NSG
- Firewalls
- VM NSG
- VMs
- Workstations

Application NSG X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

Firewalls X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

VM NSG X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

VMs X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

Workstations X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

Server B

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix.:local.net
   IPv4 Address. . . . . .:10.9.8.14
   Subnet Mask . . . . . .:255.255.255.0
   Default Gateway. . . . . .:10.10.10.1

C:\>
```

Firewall 1

Public IP: 86.210.16.10 Internal IP: 10.2.2.1

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
10.9.8.14	10.2.2.0/24	any	allow
192.2.1.0/24	10.3.9.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.2.2.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
any	any	any	block

```
fw1# show ipsec tunnels ike
IPsec Tunnel: 0
    IKE SA: ipip0    ID: 17    Version: IKEv2
        Local: 86.210.16.10[500]     Remote: 89.215.198.10[500]
        Status: DOWN

IPsec Tunnel: 1
    IKE SA: ipip1    ID: 21    Version: IKEv2
        Local: 86.210.16.10[500]     Remote: 51.187.39.9[500]
        Status: ESTABLISHED    Up: 762s    Reauth: 25278s
```

Workstation 1

```
C:\>
```

Workstation 2

```
C:\>
```

Firewall 2

Public IP: 89.215.198.10 Internal IP: 10.3.9.1

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
192.2.1.0	any	any	allow
10.2.2.0/24	10.9.8.14	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.2.2.0/24	192.2.1.11	any	allow
10.2.2.0/24	10.9.8.0/24	any	block
10.2.2.0/24	192.2.1.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
10.9.8.14	10.2.2.0/24	any	allow
10.9.8.14	192.2.1.11	any	allow
10.3.9.0/24	192.2.1.11	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
10.3.9.0/24	192.2.1.0/24	any	block
any	any	any	block

```
fw2# show ipsec tunnels ike
IPsec Tunnel: 1
    IKE SA: ipip1    ID: 53    Version: IKEv2
        Local: 89.215.198.10[500]    Remote: 43.250.192.5[500]
        Status: ESTABLISHED    Up: 2152s    Reauth: 22763s

IPsec Tunnel: 2
    IKE SA: ipip2    ID: 58    Version: IKEv1
        Local: 89.215.198.10[500]    Remote: 86.210.16.10[500]
        Status: DOWN

IPsec Tunnel: 3
    IKE SA: ipip3    ID: 60    Version: IKEv2
        Local: 89.215.198.10[500]    Remote: 52.47.73.70[500]
        Status: ESTABLISHED    Up: 11748s    Reauth: 13262s
```

Application NSG

Source	Destination	Port	Action
192.2.1.0/24	any	any	allow
10.2.2.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	block
10.9.8.14	192.2.1.0/24	any	allow
192.2.1.0/24	10.9.8.14	any	allow
192.2.1.0/24	10.2.2.0/24	any	block
192.2.1.0/24	10.3.9.0/24	any	allow
192.2.1.0/24	10.9.8.0/24	any	block
any	192.2.1.0/24	any	block

Application A

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix.:local.net
   IPv4 Address. . . . . .:192.2.1.11
   Subnet Mask . . . . . .:255.255.255.0
   Default Gateway. . . . . .:192.2.1.1

C:\>
```

VM NSG

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
192.2.1.0/24	10.3.9.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
any	10.3.9.0/24	any	block

VM 1

Answer:

下記の説明を参照してください。

Explanation:

ファイアウォール # VPNトンネルがダウンしています
オンプレミスのファイアウォール 1 とクラウド ファイアウォール 2 (ipip0/ipip2) 間の IPsec トンネルがダウンしているため、トラフィックはクラウドに通過できません。
アプリケーション NSG # ルールの構成ミス
10.3.9.0/24 # 192.2.1.0/24 には 「ブロック」ルールがあり、正当なオンプレミス クライアントがアプリケーション A に到達できないようになっています。

最新問題: **5**
ある組織の最高技術責任者 (CTO) は、IaC を使用したネットワークの変更によって予定外の障害が発生することを懸念しています。このリスクを最も効果的に軽減できる方法は次のうちどれですか。
A. マスターブランチにコード変更を加える
B. 作者による変更のコードレビューの実施
C. 変更を加える前にコードリポジトリをフォークする

D. CI/CD パイプラインにレビュー/承認ステップを追加する
Answer: (解答を表示する**)**
デプロイメント パイプラインに必須のレビューおよび承認ゲートを導入すると、すべての Infrastructure-as-Code の変更が、公開前にピアレビュー、テストされ、明示的に承認されるようになり、検証されていないコードによって予期しない停止が発生する可能性が軽減されます。

最新問題**: 6**
ネットワーク管理者は、製造工場の遠隔地にある建物を本社ビルに無線接続で接続する必要があります。無線接続の範囲を最大限に広げるために、管理者は次のうちどれを選択すべきでしょうか？ 2つ選択してください。）
A. 2.4GHz
B. 5GHz
C. 6GHz
D. 全方向性アンテナ
E. パッチアンテナ
F. 内蔵アンテナ
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
2.4GHz は、5GHz や 6GHz などの高周波数よりも範囲が広く、壁の透過性も優れています。パッチ アンテナ (指向性アンテナの一種) は信号を一方向に集中させ、建物間の長距離にわたって範囲と信頼性を大幅に向上させます。
CompTIA CloudNetX CNX-001 学習ガイドの「ワイヤレス展開とアンテナの選択」の関連抜粋:
2.4GHzは5GHzよりも広い範囲をカバーします。パッチアンテナなどの指向性アンテナは、信号をターゲットに集中させ、遠距離通信を改善します。その他のオプション：
* B および C。周波数が高いほど速度は速くなりますが、範囲は短くなります。
* D. 全方向性アンテナは信号を全方向に拡散するため、ポイントツーポイントには適していません。
* F. 内蔵アンテナは一般に利得が低く、建物間のリンクには不十分です。

最新問題**: 7**
ある企業が事業を拡大し、新たな施設を開設するにあたり、経営幹部チームは自然災害が発生した場合に施設の再建費用を補償する保険に加入することを決定しました。
次のどれがチームの決定を説明していますか?
A. 事業継続性
B. 災害復旧
C. リスク移転
D. 覚書
Answer: C (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
リスク移転とは、リスクの財務的影響を保険会社などの第三者に移転するリスク管理戦略です。このシナリオでは、自然災害による潜在的な損害や損失を補償するための保険契約の購入は、リスクを回避、軽減、または受け入れるのではなく、リスク移転の一例です。
CompTIA CloudNetX CNX-001 学習ガイドの「リスク管理の概念」の関連抜粋:
「リスク移転とは、多くの場合、保険の購入や第三者サービス契約を通じて、リスクの責任または経済的負担を第三者に移すことを指します。」このアプローチは、リスク軽減（リスクの低減）、リスク受容（リスクを許容すること）、リスク回避（リスクの排除）とは対照的です。

最新問題: **8**
悪意のある攻撃者が会社のロビーで開いているポートを利用した後、ネットワーク設計者はネットワークセキュリティを強化する必要に迫られました。ソリューションには以下の機能が必要です。
* セキュリティ態勢のチェック
* 自動修復機能
* ネットワーク分離
* デバイスとユーザーの認証
これらの要件を最もよく満たすテクノロジは次のどれですか?
A. IPS
B. マイクロセグメンテーション
C. 802.1X
D. NAC
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ネットワークアクセス制御（NAC）は、ネットワークへのアクセスを許可する前にデバイスのポスチャ（状態）を評価します。セキュリティポリシーの適用、ユーザーとデバイスの認証、非準拠デバイスの隔離または修復が可能です。
NAC は、ゲストエリアやパブリックエリアなどのネットワーク エッジでのアクセスを保護するために、エンタープライズ環境で広く使用されています。
CompTIA CloudNetX CNX-001 学習ガイドの「アクセス制御とポスチャ評価」の関連抜粋:
「NACはデバイス認証、セキュリティポスチャの検証を提供し、ポリシーコンプライアンスに基づいて自動修復または隔離アクションを実施できます。」その他のオプション：
* A. IPS は既知の脅威を検出して防止しますが、アクセス制御やポスチャ チェックは実行しません。
* B. マイクロセグメンテーションはワークロードを分離しますが、ポスチャチェックと自動修復機能がありません。

最新問題: **9**
ネットワーク アーキテクトは、次の要件を持つ新しい SD-WAN インストールの設計オプションを選択しています。
クラウドからのすべてのネットワーク トラフィックは、専用のデータ センター内の検査デバイスを通過する必要があります。
冗長性を確保します。
出力トラフィックを集中管理します。
次のネットワーク トポロジのうち、これらの要件を最もよく満たすものはどれですか。
A. ポイントツーポイント
B. ハブアンドスポーク
C. スター
D. 部分メッシュ
Answer: B (メーッセージを残す**)**
ハブアンドスポーク設計では、すべてのブランチおよびクラウドトラフィックが中央ハブ（データセンター）に送られ、検査を受けた後、再び中央ハブから出力されます。これにより、集中化された出力とセキュリティ検査の要件が満たされます。複数のハブノードを展開し、動的なパス選択を使用することで、集中化されたコントロールプレーンを失うことなく冗長性も実現できます。

最新問題: **10**
ネットワーク アーキテクトは、小売金融取引を処理する事業部を持つ大企業のために、新しいデータセンターを構築する必要があります。アーキテクトは、以下のどの情報を企業に要求すべきでしょうか？

A. 規制要件
B. 作業明細書
C. ビジネスケーススタディ
D. 内部参照アーキテクチャ
Answer: A (メーッセージを残す**)**
小売金融取引を処理する施設を設計する前に、適用されるすべてのコンプライアンスおよびセキュリティ要件（PCI DSS、SOX、GDPRなど）を理解する必要があります。これらの規制要件は、物理セキュリティ、ネットワークセグメンテーション、暗号化、ログ記録、冗長性、運用管理に関する選択を左右し、データセンターが法的義務および業界固有の義務を確実に満たすことにつながります。

最新問題**: 11**
ある企業でWi-Fiのパフォーマンスに問題が発生しています。3つのWi-Fiネットワークが利用可能で、それぞれが2.4GHz帯で同じチャンネルを使用しています。各Wi-Fiネットワークに接続すると、パフォーマンスが低下します。
ネットワークを次のどのチャネルに設定する必要がありますか?
A. チャンネル1、チャンネル2、チャンネル3
B. チャンネル2、チャンネル4、チャンネル9
C. チャンネル1、チャンネル6、チャンネル11
D. チャンネル3、チャンネル5、チャンネル10
Answer: C (メーッセージを残す**)**
これらは 2.4 GHz 帯域内の重複しない 3 つのチャネルであり、同一チャネルおよび隣接チャネルの干渉を排除して Wi-Fi パフォーマンスを最適化します。

最新問題**: 12**
ネットワークアーキテクトは、小規模教育機関の未完成のサテライトキャンパスの物理ネットワーク設計テンプレートを作成中です。新しいキャンパスは、教室を備えた2棟の小さな建物、視聴覚機器を備えた映写室1室、そして学生用座席200席で構成されます。アーキテクトは、以下のエンタープライズネットワーク設計のうち、どれを提案すべきでしょうか？
A. ハイブリッド
B. 二重層
C. 3層
D. コアが崩壊した
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
コラプスドコア設計は、コア層とディストリビューション層を単一の層に統合し、サテライトキャンパスやブランチオフィスなどの小規模ネットワークに最適です。複雑さ、コスト、フットプリントを削減しながら、必要に応じて冗長性と拡張性を維持します。
CompTIA CloudNetX CNX-001 学習ガイドの「ネットワーク設計モデル」の関連抜粋:
「小規模から中規模の導入では、コアトポロジを集約することで、基本的な機能を維持しながらハードウェアと構成の複雑さを軽減できます。」その他のオプション：
* A. ハイブリッドとは、ネットワーク トポロジではなく、クラウドと物理の融合を指します。
* B. デュアルレイヤーは標準的なエンタープライズ アーキテクチャのリファレンスではありません。
* C. 3 層は小規模ネットワークには過剰であり、不必要な複雑さを追加します。
最新問題**: 13**
ネットワーク管理者は、外部からの攻撃からネットワークを遮断するためのファイアウォールルールを設定しています。最も厳格なルールセットを作成するには、管理者は次のどれを設定する必要がありますか？

A. URLフィルタリング
B. ファイルのブロック
C. ネットワークセキュリティグループ
D. 許可リスト
Answer: D (メーッセージを残す**)**
許可リスト ポリシーでは、既知の承認済みトラフィックのみを明示的に許可し、その他のトラフィックはデフォルトでブロックすることで、最も厳格なファイアウォール ポスチャを適用します。

最新問題**: 14**
アプリケーション開発チームのユーザーがクラウド環境内のデータベースサーバーにアクセスできない問題が発生しています。他のすべてのユーザーはSSHを使用して問題なくこのサーバーにアクセスできます。ネットワークアーキテクトは、以下の情報を確認して問題のトラブルシューティングを行います。
IPAM 情報:

```
Application development gateway: 192.168.2.1/24
Application development firewall: 192.168.3.1
Server segment gateway: 192.168.1.1/24
Server segment firewall: 192.168.4.1
Database server: 192.168.1.9
Core firewall: 192.168.10.1
```

IP 192.168.2.7 が割り当てられたアプリケーション開発者のマシンからの Traceroute 出力:

```
Tracing route to 192.168.1.9 over a max of 30 hops:
1.  <1ms<1ms<1ms192.168.2.1
2.  <1ms<1ms<1ms192.168.2.2
3.   3ms  2ms  3ms192.168.1.1
4.   3ms  2ms  3ms192.168.4.1
5.    *    *    *Request Time out
6.    *    *    *Request Time out
7.    *    *    *Request Time out
```

この問題の原因として最も考えられるのは次のどれですか?
A. コアファイアウォールがトラフィックをブロックしています。
B. ネットワーク セキュリティ グループに正しい送信規則が構成されていません。
C. サーバー セグメント ファイアウォールがトラフィックをドロップしています。
D. サーバー セグメント ゲートウェイに帯域幅の問題が発生しています。
Answer: C (メーッセージを残す**)**
192.168.2.7からのtracerouteは、サーバセグメントのゲートウェイ（192.168.1.1）に到達し、その後サーバセグメントのファイアウォール（192.168.4.1）に到達しますが、データベースのサブネットには到達しません。これは、
192.168.4.1 は 192.168.1.9 へのパケットをブロックしているか転送していません。

最新問題**: 15**
クラウドネットワークエンジニアは、VPCでネットワークフロー分析を有効にして、キャプチャされたデータのヘッダーとペイロードを検査する必要があります。エ

ンジニアはこのタスクに次のどれを使用すべきでしょうか？
A. アプリケーション監視
B. Syslogサービス
C. トラフィックミラーリング
D. ネットワークフロー
Answer: C (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
トラフィックミラーリングは、ヘッダーやペイロードを含むネットワークトラフィックのコピーを分析ツールやアプライアンスに送信し、ディープパケットインスペクションを実施できるようにします。これは、クラウド環境におけるセキュリティ分析、ネットワークのトラブルシューティング、パフォーマンス診断に不可欠です。
CompTIA CloudNetX CNX-001 学習ガイドの「パケット キャプチャとネットワーク フロー モニタリング」の関連抜粋:
「トラフィックミラーリングにより、ペイロードを含む完全なパケットデータをキャプチャし、クラウドネットワーク内のフォレンジック分析やパフォーマンス分析を行うことができます。」その他のオプション：
* A. アプリケーション監視は、パケット検査ではなく、アプリレベルのメトリックに重点を置いています。
* B. Syslog はログベースであり、パケットを検査するためのものではありません。
* D. ネットワーク フロー (NetFlow、VPC フロー ログなど) はメタデータ (送信元、宛先、サイズ) を提供しますが、完全なパケットの内容は提供しません。

最新問題**: 16**
ある企業で複数のスイッチ障害が発生しています。ネットワークアナリストは次のような事実を発見しました。
ネットワークの回復時間は許容範囲を超えており、一部のスイッチのシャットダウン後に発生します。
ネットワーク内でいくつかのループが検出されました。
ブロードキャスト ストームは検出されませんでした。
次のうち、最も費用対効果の高いソリューションはどれですか?
A. 新しいレイヤー 3 スイッチを追加します。
B. 複数のVLANを追加します。
C. STP を実装します。
D. タグ付けを実装します。
Answer: C (メーッセージを残す**)**
スパニングツリープロトコルは、新しいハードウェアを必要とせずに、レイヤー2ループを防止し、自動的に解決します。また、リンクまたはスイッチ障害後のコンバージェンス時間を短縮し、回復とループ回避の要件を最もコスト効率よく満たします。

最新問題**: 17** アーキテクトは、オンプレミスでは特定の部門のみが特定のリソースにアクセスできるようにする必要があります。
同じユーザーは、キャンパスを離れた後はこれらのリソースにアクセスできません。これらの要件に従ってアクセスが確実に提供されるには、次のうちどれが適切でしょうか。
A. アクセスが必要な部門内のユーザーのみにMFAを有効にする

B. リソースのIPアドレスを使用してジオフェンシングを構成する
C. 営業時間外にこれらのリソースへのすべてのアクセスを監視するようにUEBAを構成する
D. アクセスを確保するためのPKIベースの認証システムを実装する
Answer: B (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
ジオフェンシングは、位置情報に基づいて制限を適用するネットワークアクセス制御手法です。このシナリオでは、組織はユーザーがオンプレミス（つまり、特定の物理的な場所）にいる場合にのみアクセスを許可する必要があります。ジオフェンシングは、送信元IPアドレス範囲またはGPSベースの位置情報データを使用して境界（フェンス）を定義することで実装できます。これにより、ユーザーが指定されたネットワークまたはエリア内にいる場合にのみ、特定のアプリケーションやサービスへのアクセスが許可されます。
MFA (オプション A) は ID 保証を提供しますが、物理的な場所に基づく制限は適用しません。
UEBA (オプション C) は動作分析を提供しますが、リアルタイムのアクセス制御には使用されません。
PKI (オプション D) は証明書を通じて ID 検証を提供しますが、場所を認識しません。
CompTIA CloudNetX CNX-001 公式学習ガイドからの関連抜粋:
ジオフェンシングにより、組織はユーザーの位置情報に基づいてアクセスを制限または許可する物理的または論理的な境界を定義できます。ポリシーを設定することで、ユーザーが信頼できるキャンパスまたは企業ネットワーク内にいる場合にのみアクセスを許可し、ジオフェンスエリア外からのリクエストを拒否することができます。「アクセス制御テクノロジーとID適用メカニズム」というトピックで取り上げられています。

最新問題**: 18**
管理者は、組織から外部へのメッセージやファイル転送にクレジットカード番号が含まれないようにする必要があります。次の管理策のうち、この要件を満たすものはどれですか。
A. 侵入検知システム
B. 出力フィルタリング
C. データ損失防止
D. 転送中の暗号化
Answer: (解答を表示する)
正確な抜粋からの包括的かつ詳細な説明：
データ損失防止（DLP）ソリューションは、メッセージやファイル転送をスキャンし、クレジットカード番号や社会保障番号などの機密データパターンを検出します。DLPは、組織外への情報漏洩を検知すると、ブロック、ログ記録、または警告を発します。
CompTIA CloudNetX CNX-001 学習ガイドの「データ保護とコンプライアンス管理」の関連抜粋:
「DLPシステムは、クレジットカード番号などの機密データの送信を識別して制限し、組織のデータ処理ポリシーを適用します。」その他のオプション：
* A. IDS は脅威を検出しますが、データ コンテンツ ポリシーを適用しません。
* B. 出力フィルタリングでは送信先は制限されますが、コンテンツは制限されません。
* D. 暗号化は転送中のデータを保護しますが、コンテンツのコンプライアンスは保護しません。

最新問題**: 19**
ネットワークアーキテクトは、セキュリティポリシーに基づいて組織のアプリケーションを保護するソリューションを設計しています。要件は次のとおりです。
* ユーザーは 1 セットの資格情報を使用して認証する必要があります。
* 外部ユーザーは承認されたサイトに配置する必要があります。
* セッション タイムアウトを強制する必要があります。
* ネットワーク アクセス要件は必要に応じて変更する必要があります。

これらの要件を最もよく満たすのは次のどれですか? (2 つ選択してください。)
A. ロールベースのアクセス
B. シングルサインオン
C. 静的IP割り当て
D. 多要素認証
E. 条件付きアクセスポリシー
F. リスクベース認証
Answer: B,E (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
B: シングルサインオン（SSO）- SSOは、ユーザーが統一された認証情報セットを使用して一度認証するだけで、複数のアプリケーションにアクセスできるようにします。ユーザーエクスペリエンスを向上させ、ID管理を簡素化します。
E: 条件付きアクセスポリシー - ユーザーの所在地、デバイス、リスクレベル、セッション特性に基づいて、アクセスポリシーを動的に適用できます。管理者は、承認された地域からのアクセスのみを許可したり、セッションタイムアウトを自動的に適用したり、再認証を要求したりするなどのルールを定義できます。
CompTIA CloudNetX CNX-001 学習ガイドの「アイデンティティおよびアクセス管理 (IAM)」の関連抜粋:
「SSO は、サービス間でシームレスな認証を提供し、パスワードの負担と攻撃対象領域を削減します。」
「条件付きアクセスは、位置情報、デバイスのコンプライアンス、セッションコンテキストなどのリアルタイムの条件に基づいてアクセス制御を実施し、動的なセキュリティ体制をサポートします。」その他のオプション：
* A. ロールベースのアクセスでは権限が定義されますが、場所やセッションの制御は処理されません。
* C. 静的 IP 割り当てでは、ユーザーベースのアクセス制御は提供されません。
* D. MFA はセキュリティを強化しますが、記載されているすべての要件に直接準拠しているわけではありません。
* F. リスクベースの認証では脅威のレベルを評価しますが、セッションタイムアウトや位置情報の適用を直接処理しません。

最新問題**: 20**
ある企業がクラウドベースのアプリケーションをリリースしました。一部のユーザーから、アプリケーションが読み込まれないという報告を受けています。クラウドエンジニアが問題を調査した結果、次のような報告がありました。
* すべてのユーザーがこの問題を経験しているわけではありません
* アプリケーションインフラストラクチャが最適化されている
* 問題が発生しているユーザーは、会社のリモート セールス チームに属しています。次のうち、誤って設定されている可能性が高いのはどれですか。
A. アプリケーションロードバランサー
B. ポートとプロトコル
C. IPアドレス指定
D. 地理位置情報ルール
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
アクセス問題が発生しているのはリモートセールスチームのみであり、アプリケーションインフラストラクチャは正常に動作していることが確認されているため、地理位置情報に基づくアクセス制御の設定に誤りがある可能性があります。ジオフェンシングや地域ベースの制限が誤って適用されている場合、許可された地域外のユーザーからのトラフィックが拒否される可能性があります。
CompTIA CloudNetX CNX-001 学習ガイドの「地理位置情報とアクセス制御」の関連抜粋:
位置情報ルールはIPアドレスに基づいてトラフィックをフィルタリングします。設定を誤ると、許可されていない場所からサービスにアクセスする正当なユーザーが意図せずブロックされる可能性があります。その他のオプション：

* A. ロードバランサーはトラフィックを分散し、特定のグループではなくすべてのユーザーに影響を与えます。
* B. ポート/プロトコルの誤った構成は、位置情報に基づくアクセスではなく、すべてのサービス コンポーネントまたは特定のサービス コンポーネントに影響します。
* C. IP アドレスの問題は通常、地域固有のものではなく、ネットワーク全体にわたります。

最新問題: **21**
アプリケーション開発チームのユーザーがクラウド環境内のデータベースサーバーにアクセスできない問題が発生しています。他のすべてのユーザーはSSHを使用して問題なくこのサーバーにアクセスできます。ネットワークアーキテクトは、以下の情報を確認して問題のトラブルシューティングを行います。

```
Application development gateway: 192.168.2.1/24
Application development firewall: 192.168.3.1
Server segment gateway: 192.168.1.1/24
Server segment firewall: 192.168.4.1
Database server: 192.168.1.9
Core firewall: 192.168.10.1
```

IP 192.168.2.7 が割り当てられたアプリケーション開発者のマシンからの Traceroute 出力:

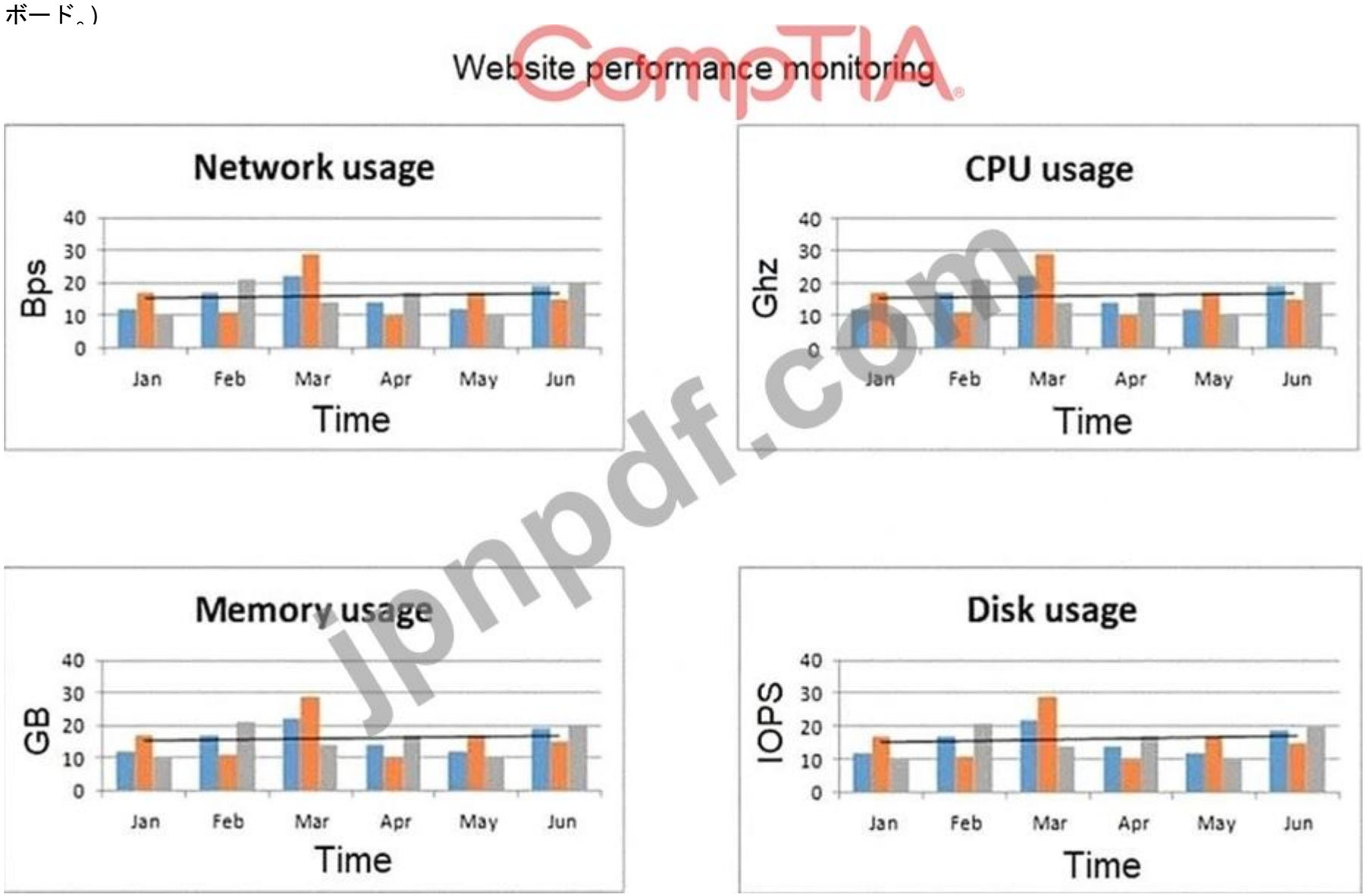
```
Tracing route to 192.168.1.9 over a max of 30 hops:
     1.  <1ms<1ms<1ms192.168.2.1
     2.  <1ms<1ms<1ms192.168.2.2
     3.   3ms  2ms  3ms192.168.1.1
     4.   3ms  2ms  3ms192.168.4.1
     5.    *    *    *Request Time out
     6.    *    *    *Request Time out
     7.    *    *    *Request Time out
```

* アプリケーション開発ゲートウェイ: 192.168.2.1/24
* サーバーセグメントゲートウェイ: 192.168.1.1/24
* データベースサーバー: 192.168.1.9
* アプリケーション開発者マシンの IP: 192.168.2.7
* トレースルートはホップ 4: 192.168.4.1 (サーバー セグメント ファイアウォール) で終了し、タイムアウトします。次のうち、この問題の原因として最も考えられるものはどれですか。

A. コアファイアウォールがトラフィックをブロックしています。
B. ネットワーク セキュリティ グループに正しい送信規則が構成されていません。
C. サーバー セグメント ファイアウォールがトラフィックをドロップしています。
D. サーバー セグメント ゲートウェイに帯域幅の問題が発生しています。
Answer: C (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
トレースルートの結果、トラフィックはアプリケーション開発ネットワーク（192.168.2.1）を正常に通過し、サーバーセグメントのゲートウェイ（192.168.1.1）を経由してサーバーセグメントのファイアウォール（192.168.4.1）に到達していることがわかります。しかし、192.168.4.1に到達した直後にタイムアウトが発生しており、このファイアウォールでトラフィックがドロップまたはフィルタリングされていることを示しています。
アプリケーション開発セグメント外の他のユーザーはデータベースサーバー（192.168.1.9）にSSH接続できるため、問題はデータベースサーバー自体やコアネット

ワークにはありません。これは、サーバーセグメントのファイアウォールがアプリケーション開発サブネット（192.168.2.0/24）からのトラフィックをブロックしていることを示しています。これは、適切なアクセスルールが定義されていない限り、セグメント化されたネットワーク設計ではよくあることです。
CompTIA CloudNetX CNX-001 学習ガイドの「ネットワーク セグメンテーションとファイアウォール ルール」の関連抜粋:
「ネットワークセグメント間のファイアウォールは、ソースに基づいてアクセスを制限するセキュリティポリシーを強制する可能性がある。
/destination IPとポート。適切な許可ルールがないと、ルーティングが成功してもトラフィックがブロックされる可能性があります。その他のオプション：
* A. コア ファイアウォールは traceroute パス内にないため、この特定のフローとは無関係です。
* B. NSG (ネットワーク セキュリティ グループ) はクラウド ワークロードに適用されますが、動作とホップバイホップのフローから、NSG の構成ミスではなく、ファイアウォール レベルの問題であることが示唆されます。
* D. 帯域幅の問題では通常、特定のホップでの一貫したタイムアウトではなく、パケット損失や高遅延が発生します。

最新問題**: 22**
電子商取引組織のネットワーク エンジニアは、Web サイトのパフォーマンスの問題により、次のダッシュボードを改善する必要があります。
(画像を参照: ネットワーク使用量、CPU 使用量、メモリ使用量、ディスク使用量などの指標を時間経過とともに表示する Web サイトのパフォーマンス監視ダッシュボード。)



運用チームのダッシュボードに追加する最も役立つ情報はどれですか?
A. 404 エラー

B. 同時ユーザー数
C. 注文数
D. アクティブなインシデントの数
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
リソース使用率指標（CPU、メモリ、ディスク、ネットワーク）は重要ですが、ユーザー需要というコンテキストが欠けています。「同時ユーザー数」を追加すると、リソース使用率の急上昇と実際のユーザー負荷を相関させることができます。Webアプリケーションのパフォーマンス監視では、同時セッション数は、パフォーマンスの問題が需要に関連しているかどうかを判断するための重要な情報を提供します。
CompTIA CloudNetX CNX-001 学習ガイドの「パフォーマンス監視とユーザー メトリック」の関連抜粋:
同時ユーザー数などのユーザー負荷指標を監視することで、パフォーマンスの低下やキャパシティプランニングに関する洞察が得られます。これらは、しきい値や自動スケーリングの要件を特定する上で非常に重要です。その他のオプション：
* A. 404 エラーはリンクが壊れていることを示しますが、パフォーマンスの問題は説明しません。
* C. 注文数はシステムの負荷ではなく、ビジネス活動を追跡します。
* D. アクティブなインシデントは、リアルタイムのパフォーマンス監視ではなく、ITSM システムに属します。

最新問題**: 23**
エンドユーザーが証明書エラーを受け取り、クラウドにデプロイされたアプリケーションに接続できません。このアプリケーションはHTTPS接続を必要とします。ネットワークソリューションアーキテクトは、エンドユーザーとクラウド内のアプリケーションの間にファイアウォールがデプロイされていることを発見しました。この問題の根本原因は次のどれですか？
A. アプリケーション サーバーのファイアウォールでポート 443 がブロックされています。
B. SSL/HTTPS 検査が有効になっているときに、ファイアウォールでポート 443 がブロックされています。
C. エンド ユーザーのラップトップには証明書がありません。
D. SSL/HTTPS 検査が有効になっていますが、ファイアウォールの証明書の有効期限が切れています。
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ファイアウォールでSSL/HTTPSインスペクションが有効になっている場合、ファイアウォールはHTTPSトラフィックを傍受して復号します。そのため、ファイアウォールはクライアントデバイスに対して独自の信頼できる証明書を提示する必要があります。その証明書の有効期限が切れている場合、クライアントブラウザに証明書エラーが表示され、アプリケーションへのアクセスがブロックされます。これは、HTTPS通信を遮断するよくある設定ミスです。
CompTIA CloudNetX CNX-001 学習ガイドの「TLS/SSL 検査と証明書管理」の関連抜粋:
SSL検査アプライアンスには有効な証明書がインストールされている必要があります。期限切れまたは信頼できない証明書がインストールされている場合、ブラウザはHTTPSセッションを拒否し、ユーザーにエラーを表示します。その他のオプション：
* A. 接続は妨げられますが、証明書エラーは発生しません。
* B. ポート 443 をブロックすると、接続はすべてブロックされますが、証明書エラーは発生しません。
* C. 相互 TLS が構成されていない限り、クライアント側の証明書は必要ありませんが、ここでは説明されていません。

最新問題**: 24**
ある企業はクラウド上でアプリケーションをホストしており、事業をヨーロッパに拡大しています。同社は一般データ保護規則（GDPR）に準拠し、ヨーロッパの顧客によるデータへのアクセスを制限する必要があります。ネットワークチームはファイアウォールルールを設定しましたが、米国の一部の顧客がヨーロッパでホストされているデータにアクセスできることがわかりました。ネットワークチームが設定すべき最適なオプションは次のうちどれですか？
A. SASE

B. ネットワークセキュリティグループ
C. CDN
D. ジオフェンシングルール
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
ジオフェンシングにより、ユーザーの IP アドレスの地理的位置に基づいてアクセス ポリシーを適用できます。
GDPR に準拠し、ユーザーの地域に基づいてアクセスを制御するには、ヨーロッパなどの特定の地域でホストされているリソースへのアクセスを制限または許可するジオフェンシングを実装する必要があります。
CompTIA CloudNetX CNX-001 学習ガイドの「データ主権と地域アクセス制御」の関連抜粋:
ジオフェンシングにより、組織は地理的なIPアドレスに基づいてデータやサービスへのアクセスを制限でき、GDPRやその他のコンプライアンスフレームワークの遵守に役立ちます。その他のオプション：
* A. SASE は、直接的なアクセス制御メカニズムではなく、より広範なフレームワークです。
* B. NSG はサブネット/NIC レベルで動作し、地理位置情報を解釈しません。
* C. CDN はデータをグローバルにキャッシュしますが、地域によるアクセスを直接制御しません。

最新問題**: 25**
ある企業は40Gbpsのネットワークを運用しており、ネットワークタップを介してIDS（侵入検知システム）でトラフィックを検査しています。サーバーがローカル更新リポジトリからパッチをダウンロードしている場合を除き、IDSは通常は正常に動作します。
10.10.10.139 に HTTPS で接続しています。パッチ適用期間中、IDS は負荷の増加に対応できず、大量のパケットをドロップします。ネットワークエンジニアがネットワークの可視性を損なうことなくこの問題を防止できる方法は、次のうちどれですか。
A. 10.10.10.139からのトラフィックを無視するようにIDSを構成する
B. PF_RING オフロードを使用して「ホスト 10.10.10.139、ポート 443」をフィルタリングします。
C. タップに「not host 10.10.10.139」BPFを追加する
D. パッチ適用期間中に IDS サービスを停止する cron ジョブをスケジュールする
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
PF_RINGは、IDSシステムが大量のトラフィックを効率的に処理できるようにする、高性能なパケットキャプチャおよびフィルタリングフレームワークです。既知の信頼できるトラフィック（パッチサーバーからのHTTPSトラフィックなど）をオフロードしてフィルタリングすることで、IDSは重要なトラフィックの分析に集中し、パケットのドロップを削減できます。
CompTIA CloudNetX CNX-001 学習ガイドの「トラフィック フィルタリングと IDS パフォーマンス最適化」の関連抜粋:
「PF_RINGのような高度なフィルタリングソリューションは、既知の信頼できるトラフィックのオフロードを可能にし、IDSシステムの処理オーバーヘッドを削減し、重要なイベントの可視性を向上させます。」その他のオプション：
* A. IDS を直接設定してトラフィックを無視すると、バイパスが多すぎて可視性に影響する可能性があります。
* C. タップ自体の BPF フィルターが、タップを使用している他のシステムに干渉する可能性があります。
* D. IDS を一時的に無効にすると、すべての可視性が失われます。これはセキュリティ上好ましくない方法です。

最新問題**: 26**
ある企業がクラウドベースのeコマースアプリケーションをホストしており、特定の場所からのみアプリケーションへのアクセスを許可したいと考えています。ネットワークチームはWAFを有効にしたクラウドファイアウォールを設定しましたが、ユーザーはグローバルにアプリケーションにアクセスできてしまいます。ネットワークチームは以下のどれを行うべきでしょうか？
A. WAFルールを再構成する

B. NATゲートウェイを設定する
C. CDNを実装する
D. 地域制限を設定する
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
Webアプリケーションファイアウォール（WAF）は、主にHTTP/HTTPSリクエストを検査し、SQLインジェクションやクロスサイトスクリプティング（XSS）攻撃などの悪意のあるトラフィックをフィルタリングするために使用されます。ただし、WAFはデフォルトでは地理的な場所に基づいてアクセスを制限することはありません。クラウドホスト型アプリケーションへのアクセスを地理的な場所に基づいて制御するには、地理的制限（ジオブロッキング）を実装するのが適切な対策です。この手法では、送信元IPの地理的な起点に基づいてクラウドベースのリソースへのアクセスを制限します。地理的制限は通常、クラウドファイアウォールまたはロードバランサーレベルで適用されます。
CompTIA CloudNetX CNX-001 公式目標からの関連抜粋:
「クラウドアクセス制御ポリシーは、地理的制限設定を適用することで、アプリケーションとサービスへのアクセスを、許可された地理的地域からのみに限定することができます。」また、「クラウド展開におけるセキュリティ制御」セクションにも記載されています。
「地理的制限は、IP 位置情報データを使用して地理的基準に基づいてサービスへのアクセスを制限し、コンプライアンスとセキュリティ要件をサポートします。」

最新問題**: 27**
ある組織は、インラインではないネットワーク監視ツールを使用してネットワークの挙動を評価したいと考えています。組織はログを使用して、潜在的な脅威の相関関係をさらに分析したいと考えています。最適なソリューションは次のうちどれですか？
A. NOC で使用される共通ダッシュボードへの Syslog
B. ログ分析機能付きSNMPトラップ
C. 事前設定されたアラートによるネットワークパケットのSSL復号化
D. SIEMに入力するNetFlow
Answer: D (メーッセージを残す**)**
NetFlowは、インラインで処理することなく、フローレベルの詳細なメタデータ（送信元/宛先IP、ポート、プロトコル、バイト数、タイムスタンプ）を提供します。これらのレコードをSIEMにエクスポートすることで、ログの一元管理が可能になり、ネットワークの挙動を他のセキュリティイベントと相関させて脅威の検出と分析を行うことができます。

最新問題**: 28**
アーキテクチャチームは、意思決定分析を実行するために、企業全体のグローバルアプリケーションで使用されるすべてのログ記録とパフォーマンス監視を統合する必要があります。この目的を達成するのに最適なテクノロジーは次のうちどれですか？
A. リレーショナルデータベース
B. コンテンツ配信ネットワーク
C. アイセス
D. データレイク
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
データレイクは、構造化データと非構造化データを大規模に集約するのに最適です。ログ、パフォーマンス指標、その他のテレメトリデータを様々なソースから保存・分析できます。データレイクは、意思決定を支援するための高度な分析と機械学習を可能にします。
CompTIA CloudNetX CNX-001 学習ガイドの「データ集約と分析」の関連抜粋:
「データレイクは、ログや監視データなど、大量かつ多様なデータの保存と分析を可能にします。企業全体の可視性と戦略的な意思決定をサポートします。」その他のオ

プション：
* A. リレーショナル データベースは構造化データに最適化されており、ログ集約のスケーラビリティが低くなります。
* B. CDN はコンテンツを配信するものであり、データの集約には使用されません。
* C. CIEM (クラウド インフラストラクチャ エンタイトルメント管理) は、ログ記録ではなくクラウドの権限を管理します。

最新問題: **29**
ネットワーク設計のセキュリティを業界のベストプラクティスに適合させるのに役立つのは次のどれですか?
A. リファレンスアーキテクチャ
B. ライセンス契約
C. サービスレベル契約
D. 覚書
Answer: (解答を表示する**)**
リファレンス アーキテクチャは、セキュリティに関する業界のベスト プラクティスを組み込んだ、標準化されたベンダーに依存しないブループリントを提供し、ネットワーク設計が実証済みのフレームワークに準拠していることを保証します。

最新問題: **30**
ネットワーク管理者は、社内ネットワークに接続できないユーザーのワークステーションのトラブルシューティングを行っています。ipconfigとarp -aの結果が表示されています。ユーザーのワークステーションは次の状態です。

```
c:\>ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet 1:
   Physical Address. . . : 1A-21-11-33-44-5A
   DHCP Enabled. . . . . : Yes
   IPv4 Address. . . . . : 10.21.12.8
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . : 10.21.12.254
```

同じネットワーク上のルータでは次の出力が表示されます。

```
#arp -a
Internet Address          Physical Address
  10.21.12.254            12-34-56-78-9a-bc
  10.21.12.255            ff-ff-ff-ff-ff-ff
  10.21.12.2              1A-21-11-2F-1E-11
  10.21.12.3              1A-21-11-1B-2C-44
  10.21.12.8              1A-21-11-31-74-4C
  10.21.12.10             1A-21-11-43-10-BB
```

* IPアドレスは10.21.12.8です
* サブネットマスクは255.255.255.0です
* デフォルトゲートウェイは10.21.12.254です
* ARPテーブルには、10.21.12.8が1A-21-11-31-74-4C（ローカルアダプタとは異なるMACアドレス）にマッピングされていることが示されています。

A. 非同期ルーティング
B. IPアドレスの競合
C. DHCPサーバーがダウンしています
D. ブロードキャストストーム
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
ローカルマシンのIPアドレスは10.21.12.8、物理アドレスは1A-21-11-33-44-5Aです。しかし、ARPテーブルを見ると、10.21.12.8は別のMACアドレス（1A-21-11-31-74-4C）にマッピングされています。これは、ネットワーク上の別のデバイスが同じIPアドレスに対するARP要求に応答していることを意味します。これは明らかにIPアドレスの競合を示しており、ワークステーションがネットワーク上で正常に動作しなくなる可能性があります。
CompTIA CloudNetX CNX-001 学習ガイドの「IP アドレスの問題のトラブルシューティング」からの関連抜粋:
「IP競合は、同じネットワーク上の2つのデバイスに同じIPアドレスが割り当てられている場合に発生します。症状としては、接続の切断、ARPエントリの重複、ルーティング動作の不一致などがあります。」その他のオプション：
* A. 非同期ルーティングとは、パケットが異なる戻りパスを取ることを指し、ARP の不整合とは無関係です。
* C. DHCP サーバーの問題は IP 割り当てに影響しますが、ここには示されていません。ワークステーションには IP アドレスが割り当てられています。

最新問題: **31**
ネットワークエンジニアは、既存のインフラストラクチャを置き換えるため、データセンターに新しいスイッチを設置しています。以前のネットワークハードウェアには、同じサブネット上の他のすべてのサーバーハードウェアと同様に、既存のネットワークに接続された管理インターフェースがありました。これらの管理インターフェースのセキュリティを強化するために、エンジニアは次のうちどれを行うべきでしょうか？
A. スイッチ管理ポートを別の物理ネットワークに接続します。
B. スイッチ上の未使用の物理ポートを無効にして、権限のないユーザーのアクセスを防止します。
C. 管理インターフェイスとネットワーク スイッチ ポートを同じ VLAN に設定します。
D. すべてのスイッチファームウェアを最新のハードウェア レベルにアップグレードします。
Answer: A (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
管理インターフェースのセキュリティを強化するためのベストプラクティスは、管理ポートを専用の管理ネットワークに接続し、本番ネットワークから分離することです。これにより、本番サブネット上のデバイスやユーザーからの不正アクセスを防ぎ、攻撃対象領域を縮小できます。
CompTIA CloudNetX CNX-001 学習ガイドの「ネットワーク インフラストラクチャのセキュリティ保護」の関連抜粋:
「管理インターフェースは、ユーザーとデータのトラフィックから物理的および論理的に分離できる、別の帯域外管理ネットワークに配置する必要があります。」これにより、管理ネットワーク上の信頼できるデバイスのみが管理インターフェースにアクセスできるようになります。
その他のオプション:
* B. 未使用のポートを無効にするのは良い方法ですが、管理トラフィックの分離には対処できません。
* C. 管理インターフェースと本番トラフィックを同じ VLAN に配置すると、潜在的な内部脅威にさらされることになります。
* D. ファームウェアのアップグレードはセキュリティ パッチにとって重要ですが、インターフェイスを分離するものではありません。

最新問題: **32**
経理部門がレポートを作成している時間帯に、営業チームでビデオ会議のパフォーマンスに問題が発生しています。次のうち、最適な解決策はどれですか？
A. 業務時間外に経理部門のレポートを実行する
B. ロードバランサーを使用してビデオトラフィックを均等に分割する
C. 企業ネットワークスイッチでのQoSの設定
D. ハイエンドスイッチを購入してネットワークのスループットを向上させる
Answer: C (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
QoS（Quality of Service）は、ビデオ会議のような遅延の影響を受けやすいトラフィックを、レポート生成のような帯域幅を多く消費するが遅延が許容されるタスクよりも優先的に処理します。ネットワークスイッチにQoSを実装することで、ネットワークはトラフィックの種類を区別し、輻輳時にも重要なアプリケーションに十分な帯域幅を確保できます。
CompTIA CloudNetX CNX-001 学習ガイドの「トラフィックの優先順位付けと QoS」の関連抜粋:
「QoSは、ネットワークトラフィックの分類と優先順位付けを可能にし、音声やビデオなどのミッションクリティカルなアプリケーションやリアルタイムアプリケーションのパフォーマンスを確保します。」その他のオプション：
* A. 営業時間外にタスクをスケジュールすることは、拡張性や信頼性に欠けます。
* B. 負荷分散はサーバーに適用され、LAN トラフィックの優先順位付けには適用されません。
* D. ハイエンドのスイッチを購入するとコストがかかり、負荷がかかった状態で競合を解決できない可能性があります。

最新問題: **33**
あるカフェではタブレット端末を使ったPOSシステムを導入しています。お客様から、料理の提供に時間がかかりすぎるという苦情が寄せられています。調査の結果、以下の点が判明しました。
* すべてのキッチンプリンターが注文を印刷したわけではない
* 支払いは正常に処理されています
* クラウドベースのシステムには注文の記録が保存されます
* この問題はカフェが混雑していたときに発生しました
この問題を軽減するための最善の方法は次のどれですか?
A. アプリケーションの更新
B. キッチン専用のアクセスポイントの追加
C. キッチンプリンターのワイヤレスドングルのアップグレード
D. キッチンプリンターに静的IPアドレスを割り当てる
Answer: (解答を表示する)
正確な抜粋からの包括的かつ詳細な説明：
決済は機能しており、注文はクラウドに記録されているため、問題はタブレットとキッチンプリンター間のローカル無線ネットワークにあると考えられます。問題が使用量の多い時間帯にのみ発生する場合は、混雑または信号品質の問題である可能性があります。キッチン専用のアクセスポイントを追加することで、プリンターのトラフィックを分離し、信頼性を向上させることができます。
CompTIA CloudNetX CNX-001 学習ガイドの「ワイヤレス パフォーマンスと干渉管理」の関連抜粋:

「トラフィックをセグメント化したり、ミッションクリティカルなデバイス専用のAPを導入することで、競合を軽減し、混雑した無線環境における信頼性を確保できます。」その他のオプション：
* A. アプリのアップデートでは無線干渉は修正されません。
* C. ドングルのアップグレードは役立つかもしれませんが、トラフィックを分離することはできません。
* D. 静的 IP はアドレス指定には役立ちますが、ワイヤレスの信頼性には役立ちません。

最新問題**: 34**
ユーザーからデータベースサーバーへの接続に関する問題が報告されました。このデータベースのフロントエンドアプリケーションは、会社のWebサーバーでホストされています。ネットワークエンジニアは、会社のサーバーが配置されているネットワークサブネットとサーバーのIPアドレスを変更しました。新しい構成は次のとおりです。
* サーバーの新しいサブネットは 10.10.10.64/27 です
* WebサーバーのIPアドレスは10.10.10.101です
* データベースサーバーのIPは10.10.10.93です
ユーザーの問題の原因として最も可能性が高いのは次のどれですか?
A. Web アプリケーション サーバーは要求を転送していません。
B. データベース サーバーのファイアウォールがデータベースへのポートをブロックしています。
C. DNS サーバーが正しく解決されていません。
D. Web サーバーのネットワーク構成が正しくありません。
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
サブネットとIPアドレスが最近変更され、ユーザーがWebアプリケーション経由でデータベースにアクセスしているため、DNSレコードが新しいIPアドレスを反映するように更新されていないことが問題と考えられます。DNSが古いIPアドレスを参照している場合、新しいサブネット上でサービスが稼働していてアクセス可能であっても、ユーザーはサービスにアクセスできません。
CompTIA CloudNetX CNX-001 学習ガイドの DNS およびネットワーク構成のトラブルシューティング」からの関連抜粋:
IPアドレスの変更後には、DNSの設定ミスがよくある問題となります。DNSエントリが適切に更新されない場合、クライアントは古いIPアドレスでサービスにアクセスしようとします。その他の選択肢：
* A. Web サーバーの構成ミスを示す兆候は提供されません。
* B. ファイアウォールの問題は、1 人のユーザーだけでなく、すべてのユーザーに影響します。
* D. Web サーバーの IP アドレスはサブネット範囲内にあり、誤った構成は示されていません。

最新問題**: 35**
クラウドエンジニアは、クラウド移行のためにパブリッククラウド環境でVMを構築する計画を立てています。クラウドセキュリティポリシーにより、新規VM構築時のコンソールへのアクセスが制限されています。エンジニアは、ネットワーク設定が事前に構成されていることを確認するために、各VMの設定を複製したいと考えています。最適な展開方法は次のうちどれですか？
A. IaC テンプレート
B. カスタムSDK
C. APIスクリプト
D. CLIコマンド
Answer: A (メーッセージを残す**)**

Infrastructure-as-Code テンプレートを使用すると、ネットワーク設定を含むすべての VM 構成を、展開時に自動的に適用されるコードで定義およびバージョン管理できるため、コンソールの変更が不要になり、各ビルド間の一貫性が確保されます。

最新問題: **36**
ある企業は40Gbpsのネットワークを運用しており、ネットワークタップを介してIDS（侵入検知システム）でトラフィックを検査しています。サーバーがローカル更新リポジトリからパッチをダウンロードしている場合を除き、IDSは通常は正常に動作します。
10.10.10.139 に HTTPS で接続しています。パッチ適用期間中、IDS は負荷の増加に対応できず、大量のパケットをドロップします。ネットワークエンジニアがネットワークの可視性を損なうことなくこの問題を防止できる方法は、次のうちどれですか。
A. 10.10.10.139からのトラフィックを無視するようにIDSを構成する
B. PF_RING オフロードを使用して「ホスト 10.10.10.139、ポート 443」をフィルタリングします。
C. タップに「host 10.10.10.139」BPFを追加する
D. パッチ適用期間中に IDS サービスを停止する cron ジョブをスケジュールする
Answer: C (メーッセージを残す**)**
Berkeley Packet Filter を適用して、IDS に到達する前に HTTPS patch#repo トラフィックのみをドロップすることで、パッチ ウィンドウ中の処理の負担を軽減しながら、他のすべてのフローの完全な可視性を維持します。
これにより、IDS 自体の再構成や、ネットワークの残りの部分での可視性の喪失が回避されます。

最新問題: **37**
ネットワーク管理者は、リモートサイトで発生した障害のトラブルシューティングを行っています。ログを調べたところ、サイトのインターネットリンクの1つがダウンしていることが判明しました。サービスプロバイダがこの情報を確認した後、管理者はトラフィックをバックアップリンクにフェイルオーバーしました。次に、管理者は次のうちどれを行うべきでしょうか？
A. 学んだ教訓を文書化します。
B. 行動計画を立てます。
C. 問題を特定します。
D. システムの全機能を検証します。
Answer: D (メーッセージを残す**)**
フェールオーバー ソリューションを実装した後、チケットを閉じる前に、すべてのサービスとネットワーク パスが完全に復元され、正しく動作していることを確認する必要があります。

最新問題: **38**
あるコールセンター会社は、VoIPインフラを通じてサービスを提供しています。最近、クラウドアプリケーション上でドキュメントを管理するアプリケーションを導入しました。このアプリケーションが原因で、VoIP発信者の音声が頻繁に途切れています。ネットワーク管理者は、最も費用のかからない解決策でこの問題を解決する必要があります。次のうち、最適なアプローチはどれですか？
A. 2つ目のインターネットリンクを追加し、音声とデータネットワークを物理的に異なるルートに分割する
B. インターネットルータでQoSルールを設定してVoIP通話を優先する
C. 音声用とデータ用の2つのVLANを作成する
D. より高い圧縮率の音声コーデックを使用するようにVoIPデバイスを設定する
Answer: B (メーッセージを残す**)**
ドキュメント管理トラフィックよりも VoIP パケットを優先することで、ネットワークが混雑している場合でも音声に必要な帯域幅と低遅延が確保されます。新しいリンクやハードウェアのコストは一切かかりません。

最新問題: **39**
ネットワークアーキテクトは、複数のプライベートデータセンターを接続するための新しいネットワークを設計する必要があります。ネットワークには以下の要件があります。
拠点間のすべてのトラフィックにプライバシーを提供します。
既存のインターネット接続を使用します。
最適なパス上でアプリケーション トラフィックのインテリジェントなステアリングを使用します。
これらの要件を最もよく満たすのは次のどれですか?
A. MPLS接続
B. SD-WAN
C. サイト間VPN
D. エクスプレスルート
Answer: B (メーッセージを残す**)**
SD-WAN ソリューションは、既存のインターネット リンク上で暗号化されたトンネルを実行し、最適なパスを介してトラフィックを動的に誘導することで、新しいプライベート回線を必要とせずにプライバシーとパフォーマンス インテリジェンスを実現します。

最新問題: **40**
ある組織は、インラインではないネットワーク監視ツールを使用してネットワークの挙動を評価したいと考えています。組織は、ログを使用して潜在的な脅威の相関関係をさらに分析したいと考えています。最適なソリューションは次のうちどれですか？
A. NOC で使用される共通ダッシュボードへの Syslog
B. ログ分析機能付きSNMPトラップ
C. 事前設定されたアラートによるネットワークパケットのSSL復号化
D. SIEMに入力するNetFlow
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
NetFlowは、インライン実装を必要とせずに、IPトラフィックに関するフローレベルのメタデータを提供します。誰が誰とどのくらいの時間通信し、どれだけのデータ交換があったかを要約します。SIEMに送信して相関分析を行うことで、動作監視や脅威検出に最適です。
CompTIA CloudNetX CNX-001 学習ガイドの 「NetFlow とネットワーク テレメトリ」の関連抜粋:
NetFlowはトラフィックパターンの可視性を提供し、SIEMプラットフォームと統合することで異常検出やセキュリティ分析に活用できます。その他のオプション：
* A. Syslog にはイベント レベルのデータが表示されますが、ネットワークの動作は表示されません。
* B. SNMP トラップはトラフィックの動作ではなく、デバイスの状態を監視します。
* C. SSL 復号化は複雑であり、インライン配置が必要です。

最新問題: **41**
あるグローバル企業は、様々な場所に拠点を置いています。各拠点には独自のアプリケーションがローカルに導入されていましたが、統合されたデータを即座に取得できない問題が発生しました。最高情報責任者 (CIO) は、アプリケーションを一元管理し、クラウドに導入することを決定しました。クラウド導入後、ユーザーからアプリケーションの速度が遅いという報告がありました。最も考えられる問題は次のうちどれですか？
A. スロットリング
B. 過剰利用
C. パケットロス
D. レイテンシー

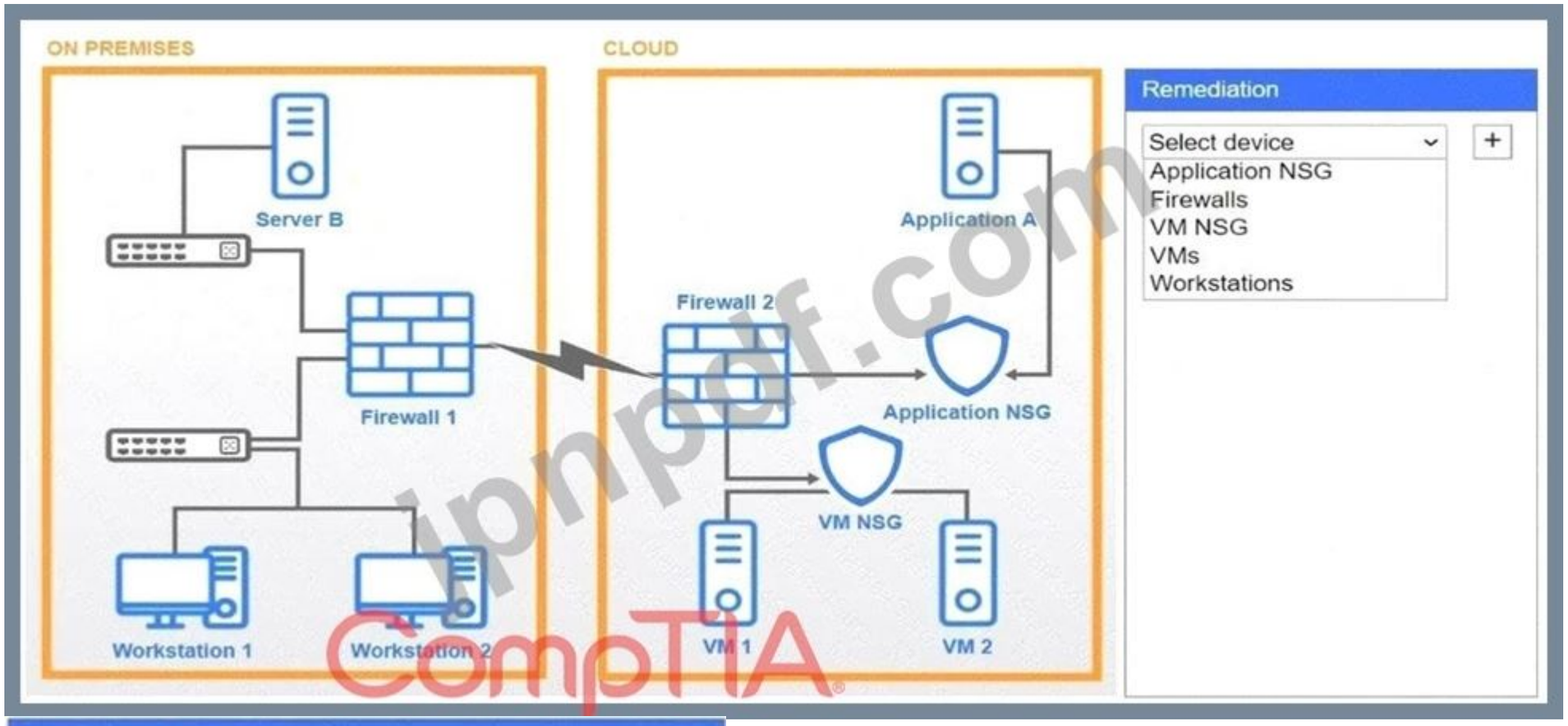
Answer: D (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
アプリケーションをローカル環境から集中型のクラウド環境に移行する場合、リモートユーザーはWAN経由で接続する必要があります。アプリケーションが遅延の影響を受けやすい場合、特に地理的に分散した地域間では、レイテンシが大きな問題となります。これは、リモートオフィスにサービスを提供する集中型アプリケーションに共通するパフォーマンス上の懸念事項です。
CompTIA CloudNetX CNX-001 学習ガイドの 『クラウド パフォーマンスと WAN 接続」の関連抜粋:
『リモート ユーザーがアクセスするクラウド ホスト アプリケーションでは、遅延に関連するパフォーマンスの問題が発生する可能性があります。
最適化戦略には、CDN、キャッシュ、エッジ展開などが含まれる場合があります。
その他のオプション:
* A. スロットリングは通常、帯域幅またはレート制限のことを指し、全体的な速度低下のことを指すものではありません。
* B. 過剰利用の可能性はあるが、インフラは集中化され新しいものになると言われている。
* C. パケット損失により、速度低下だけでなく、切断や障害が発生する可能性が高くなります。

最新問題**: 42**
セキュリティアーキテクトは、コンピュータハードウェアの設置に関するセキュリティ管理を強化する必要があります。要件は次のとおりです。
コンピュータ室への監査可能なアクセスログ
不正アクセスの試みに関するアラート
コンピュータ室内のリモート可視性
次のコントロールのうち、これらの要件を最もよく満たすものはどれですか? (2 つ選択してください。)
A. ビデオ監視
B. NFCアクセスカード
C. モーションセンサー
D. 錠前と鍵
E. 警備パトロール
F. 自動照明
Answer: A,B (メーッセージを残す)
ビデオ監視により、コンピュータ ルームへの継続的なリモート ビジビリティが提供され、分析機能と統合して不正な存在に関するアラートを生成することもできます。
NFC アクセス カードは、すべてのカード スワイプを記録し、失敗した場合や時間外の試行に対してアラートを発行するシステムを使用して制御された入場を強制し、監査可能なアクセス レコードと疑わしいアクティビティの即時通知を提供します。

最新問題**: 43**
ネットワーク アーキテクトは、次の要件を持つ新しい SD-WAN インストールの設計オプションを選択しています。
* クラウドからのすべてのネットワーク トラフィックは、専用のデータセンター内の検査デバイスを通過する必要があります。
* 冗長性を確保する。
* 出力トラフィックを集中管理します。
次のネットワーク トポロジのうち、これらの要件を最もよく満たすものはどれですか。
A. ポイントツーポイント
B. ハブアンドスポーク
C. スター

D. 部分メッシュ
Answer: B (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ハブアンドスポーク トポロジは、ブランチ オフィスまたはクラウド ワークロードからのトラフィックを検査、監視、またはセキュリティの適用のために中央の場所 (ハブ) 経由でルーティングする必要がある SD-WAN 環境に最適です。
この構造により、出力が一元化され、ハブを介した冗長スポークパスが可能になります。また、制御が簡素化され、コンプライアンスポリシーの適用も容易になります。
CompTIA CloudNetX CNX-001 学習ガイドの「SD-WAN トポロジとクラウド出力戦略」の関連抜粋:
ハブアンドスポークトポロジでは、スポーク（リモートオフィスまたはクラウドノード）が中央ハブを介して接続され、集中的な出力、トラフィック検査、および簡素化されたルーティングが可能になります。その他のオプション：
* A. ポイントツーポイントは拡張性がなく、集中管理ができません。
* C. スター トポロジはハブ アンド スポークに似ていますが、より堅牢で、SD-WAN のスケーラビリティには適していません。
* D. 部分メッシュにより、集中検査を回避して、スポーク間の直接通信が可能になります。

最新問題**: 44**
ネットワーク管理者は、ハイブリッドクラウド環境における接続の問題を解決する必要があります。ワークステーションとVMはアプリケーションAにアクセスできません。ワークステーションはサーバーBにアクセスできます。
説明書
ワークステーション、VM、ファイアウォール、NSG をクリックしてトラブルシューティングを行い、情報を収集します。ターミナルに「help」と入力すると、使用可能なコマンドの一覧が表示されます。
修復が必要な適切なデバイスを選択し、関連する問題を特定します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

VM NSG X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

VMs X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

Workstations X

Issue:

- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

Firewall 1

Public IP: 86.210.16.10 Internal IP: 10.2.2.1

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
10.9.8.14	10.2.2.0/24	any	allow
192.2.1.0/24	10.3.9.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.2.2.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
any	any	any	block

```
fw1# show ipsec tunnels ike
IPsec Tunnel: 0
    IKE SA: ipip0    ID: 17    Version: IKEv2
        Local: 86.210.16.10[500]    Remote: 89.215.198.10[500]
        Status: DOWN

IPsec Tunnel: 1
    IKE SA: ipip1    ID: 21    Version: IKEv2
        Local: 86.210.16.10[500]    Remote: 51.187.39.9[500]
        Status: ESTABLISHED    Up: 762s    Reauth: 25278s
```

Workstation 1

```
C:\>
```

Workstation 2

```
C:\>
```


Firewall 2

Public IP: 89.215.198.10 Internal IP: 10.3.9.1

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
192.2.1.0	any	any	allow
10.2.2.0/24	10.9.8.14	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.2.2.0/24	192.2.1.11	any	allow
10.2.2.0/24	10.9.8.0/24	any	block
10.2.2.0/24	192.2.1.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
10.9.8.14	10.2.2.0/24	any	allow
10.9.8.14	192.2.1.11	any	allow
10.3.9.0/24	192.2.1.11	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
10.3.9.0/24	192.2.1.0/24	any	block
any	any	any	block

```
fw2# show ipsec tunnels ike
IPsec Tunnel: 1
    IKE SA: ipip1    ID: 53    Version: IKEv2
        Local: 89.215.198.10[500]    Remote: 43.250.192.5[500]
        Status: ESTABLISHED    Up: 2152s    Reauth: 22763s

IPsec Tunnel: 2
    IKE SA: ipip2    ID: 58    Version: IKEv1
        Local: 89.215.198.10[500]    Remote: 86.210.16.10[500]
        Status: DOWN

IPsec Tunnel: 3
    IKE SA: ipip3    ID: 60    Version: IKEv2
        Local: 89.215.198.10[500]    Remote: 52.47.73.70[500]
        Status: ESTABLISHED    Up: 11748s    Reauth: 13262s
```

Application NSG

Source	Destination	Port	Action
192.2.1.0/24	any	any	allow
10.2.2.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	block
10.9.8.14	192.2.1.0/24	any	allow
192.2.1.0/24	10.9.8.14	any	allow
192.2.1.0/24	10.2.2.0/24	any	block
192.2.1.0/24	10.3.9.0/24	any	allow
192.2.1.0/24	10.9.8.0/24	any	block
any	192.2.1.0/24	any	block

Application A

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix.:local.net
   IPv4 Address. . . . . .:192.2.1.11
   Subnet Mask . . . . . .:255.255.255.0
   Default Gateway. . . . . .:192.2.1.1

C:\>
```

VM NSG

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
192.2.1.0/24	10.3.9.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
any	10.3.9.0/24	any	block

Answer:

下記の説明を参照してください。

Explanation:

ファイアウォール＃VPNトンネルがダウンしています

オンプレミスのファイアウォール 1 とクラウド ファイアウォール 2 (ipip0/ipip2) 間の IPsec トンネルがダウンしているため、トラフィックはクラウドに通過できませ

ん。
アプリケーション NSG # ルールの構成ミス
10.3.9.0/24 # 192.2.1.0/24 には 「ブロック」ルールがあり、正当なオンプレミス クライアントがアプリケーション A に到達できないようになっています。

最新問題: **45**
コアスイッチのソフトウェアアップグレード後に障害が発生しました。ネットワーク管理者は、インストールされたファームウェアにバグがあったと考えています。
ネットワーク管理者は次に、次のうちどの対応を行うべきでしょうか？
A. 学んだ教訓を文書化します。
B. ソリューションを実装します。
C. 問題を解決するための行動計画を立てます。
D. 原因を特定するために理論をテストします。
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
CNX-001の目標で概説されている構造化されたトラブルシューティング手法によれば、潜在的な根本原因（この場合はファームウェアのバグの疑い）が特定されたら、次のステップは、対策を講じる前に、その理論を検証して原因を確認することです。これにより、誤診や不要な設定変更を防ぐことができます。
CompTIA CloudNetX CNX-001 学習ガイドの「構造化トラブルシューティング方法論」の関連抜粋:
症状を特定し、考えられる原因の理論を構築した後、次のステップは、その理論を検証し、それが問題の実際の原因であることを確認することです。その他の選択肢：
* A. 原因を確認した後、行動計画を立てます。
* C. 学んだ教訓を文書化することが最後のステップです。
* D. 問題が確認された後にのみ、解決策を実装する必要があります。

最新問題: **46**
ネットワーク セキュリティ管理者は、次のソリューションを設定する必要があります。
* ログ ファイルからすべてのデータを 1 つの場所に収集します。
* データを相関させてアラートを生成します。
管理者は次のどれを実装する必要がありますか?
A. Syslog
B. イベントログ監視
C. ログ管理
D. 見る
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
SIEM（セキュリティ情報イベント管理）ソリューションは、複数のソースからログデータを取り込み、イベントを相関分析し、異常を検知し、事前定義または動的なルールに基づいてアラートを生成します。そのため、SIEMは集中ログ記録とリアルタイムの脅威検知に最適なソリューションです。
CompTIA CloudNetX CNX-001 学習ガイドの「セキュリティ監視とログ相関」の関連抜粋:
「SIEMプラットフォームは、多様なソースからのログを集約、正規化、分析し、リアルタイムのアラートとインシデント対応サポートを提供します。」その他のオプション：
* A. Syslog はトランスポート プロトコルであり、相関関係や警告は生成しません。
* B. イベント ログの監視は個々のシステムに制限されます。
* C. ログ管理ではログが保存されますが、分析やアラートは実行されません。

最新問題: **47**
ネットワークロードバランサーがクライアントのTLS証明書を正しく検証していません。ネットワークアーキテクトは、ロードバランサーにインストールされている証明書を検証してから、次のステップに進む必要があります。秘密鍵と証明書が一致しているかどうかを確認するために、アーキテクトは次のコマンドのどれを使用すべきでしょうか？
A. openssl-list -noout -modulus -in cert.crt | openssl md5
openssl rsa -noout -modulus -in privkey.txt | openssl md5
B. openssl req -in certificate.csr -verify
openssl-verify -noout -modulus -in privkey.txt | openssl md5
C. openssl-rsa -noout -modulus -in cert.crt | openssl md5
openssl-verify -noout -modulus -in privkey.txt | openssl md5
D. openssl x509 -noout -modulus -in cert.crt | openssl md5
openssl rsa -noout -modulus -in privkey.txt | openssl md5
Answer: D (メーッセージを残す**)**
MD5 ハッシュが一致する場合、証明書と秘密キーは正しく対応しています。

最新問題: **48**
ネットワークセキュリティエンジニアは、パブリッククラウド内の仮想マシン上で実行されているウェブアプリケーションのセキュリティを確保する必要があります。仮想マシンはアプリケーションロードバランサーの背後に配置されています。エンジニアは、仮想マシンのセキュリティを確保するために、以下のどのテクノロジーを使用すべきでしょうか？ 2つ選択してください。）
A. CDN
B. DLP
C. IDS
D. WAF
E. 見る
F. NSG
Answer: D,F (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
WAF（Webアプリケーションファイアウォール）は、アプリケーションとの間のHTTP/Sトラフィックを検査することで、Webアプリケーションを保護します。悪意のあるトラフィックや、Webアプリケーションの脆弱性を狙ったエクスプロイトをフィルタリング、監視、ブロックします。WAFはエッジに導入され、多くの場合ロードバランサーと組み合わせて利用され、SQLインジェクション、クロスサイトスクリプティング、プロトコル違反などの脅威を軽減するのに最適です。
NSG（ネットワーク セキュリティ グループ）は、多くのクラウド プロバイダー（Azure など）が提供するネイティブ セキュリティ機能であり、ファイアウォールと同様に機能します。NSG は、仮想ネットワーク インターフェイス、サブネット、または VM レベルで受信トラフィックと送信トラフィックを制御し、エンジニアが許可または拒否するトラフィック ルールを定義できるようにします。

CompTIA CloudNetX CNX-001 学習ガイドの「クラウド ワークロード保護とセキュリティ ツール」からの関連抜粋:
「WAF は、パブリック クラウド環境で Web 対応アプリケーションを保護するために不可欠です。」
「ネットワーク セキュリティ グループ (NSG) は、クラウドベースの仮想ネットワークにアクセス ポリシーを適用するために使用され、インスタンス レベルまたはサブネット レベルでフィルタリングとセグメンテーションを提供します。」

最新問題: **49**
ネットワーク管理者は、会社のオフィスから、ビデオ通話が1分間は正常に動作するものの、その後途切れ途切れになるという問い合わせを受けました。ネットワーク管理者は、そのオフィスからビデオサーバーにpingを送信し、接続可能であることを確認しました。

```
Ping 10.172.16.16
Pinging 10.172.16.16 with 32 bytes of data:
Reply from 10.172.16.16: bytes=32 time=40ms TTL=53
Reply from 10.172.16.16: bytes=32 time=11ms TTL=53
Reply from 10.172.16.16: bytes=32 time=672ms TTL=53
Reply from 10.172.16.16: bytes=32 time=111ms TTL=53
Reply from 10.172.16.16: bytes=32 time=117ms TTL=53
Reply from 10.172.16.16: bytes=32 time=849ms TTL=53
Reply from 10.172.16.16: bytes=32 time=34ms TTL=53
Reply from 10.172.16.16: bytes=32 time=92ms TTL=53
```


ビデオ通話の問題の原因として最も可能性が高いのは次のどれですか?
A. スループット
B. ジッター
C. レイテンシー
D. 敗北
Answer: B (メーッセージを残す)
ping応答時間が大きく変動する（11ミリ秒から849ミリ秒まで）のは、パケット遅延の変動が大きいことを示しており、その結果、ビデオストリームが短時間で途切れ途切れになることがあります。この遅延の変動はジッターと呼ばれます。

最新問題: **50**
ネットワーク アーキテクトは、次の要件を満たす新しいブランチ ネットワークを設計する必要があります。
* 単一障害点なし
* クライアントは基盤となるメディアの変更による影響を受けません
* 帯域幅を節約するためにクライアントは直接通信できる必要があります
アーキテクトは次のどのネットワーク トポロジを使用する必要がありますか?
A. ハブアンドスポーク
B. メッシュ
C. 背表紙付き
D. スター
Answer: B (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
メッシュトポロジーは、すべてのノード間に複数の冗長パスを提供し、単一障害点を排除します。クライアントは中央ハブを経由することなく相互に直接通信できるため、ボトルネックが軽減され、帯域幅を節約できます。メッシュネットワークはフォールトトレランス性に優れ、基盤となるメディアの変化にも柔軟に対応できるため、高可用性が求められる分散環境に最適です。

CompTIA CloudNetX CNX-001 学習ガイドの「WAN および LAN トポロジ」の関連抜粋:
メッシュトポロジでは、すべてのデバイスが他のすべてのデバイスに接続されます。この設計はフォールトトレランスを提供し、エンドポイント間の直接通信パスを可能にするため、帯域幅効率が最大化され、単一障害点が排除されます。その他のオプション：
* A. ハブアンドスポークでは、中央の障害点が発生し、帯域幅が制限される可能性があります。
* C. スパイン&リーフはデータ センターには最適ですが、ブランチ オフィスの設計には通常使用されません。
* D. スター トポロジは中央スイッチに依存し、単一障害点があります。

最新問題**: 51**
ある企業でWi-Fiのパフォーマンスに問題が発生しています。3つのWi-Fiネットワークが利用可能で、それぞれが2.4GHz帯で同じチャンネルを使用しています。各Wi-Fiネットワークに接続すると、パフォーマンスが低下します。
ネットワークを次のどのチャネルに設定する必要がありますか?
A. チャンネル1、チャンネル2、チャンネル3
B. チャンネル2、チャンネル4、チャンネル9
C. チャンネル1、チャンネル6、チャンネル11
D. チャンネル3、チャンネル5、チャンネル10
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
2.4GHz帯のWi-Fiでは、周波数スペクトルの分割方法によりチャネルが重複します。同一チャネル干渉および隣接チャネル干渉を防ぐため、重複しないチャネルのみを使用する必要があります。IEEE 802.11規格およびCompTIA CloudNetX CNX-001学習ガイドに記載されているベストプラクティスによれば、
「ワイヤレス ネットワークの最適化」では、2.4 GHz 帯域内の重複しない 3 つのチャネルは次のとおりです。
* チャネル1 （2.412GHz）
* チャネル6 （2.437GHz）
* チャネル11 （2.462GHz）
これらのチャネルは、近接して動作する場合でも干渉を回避できるほど十分に間隔が空けられています。
重複するチャネル (オプション A、B、D など) を使用すると、競合と再送信が増加するため、信号が劣化し、パフォーマンスが低下します。
CompTIA CloudNetX CNX-001 からの関連抜粋:
「2.4 GHz 帯域で動作する Wi-Fi ネットワークでは、複数のアクセス ポイントがある環境で最大のスループットと最小の干渉を確保するために、チャネル 1、6、および 11 を使用する必要があります。」

最新問題**: 52**
ネットワーク アーキテクトは、データ センター内のラックにネットワーク コア機器を配置するソリューションを設計しています。
この機器は企業にとって極めて重要であり、誰かがネットワークコアに直接接続する可能性を最小限に抑えるため、可能な限りセキュリティを確保する必要があります。現在のセキュリティ設定は次のとおりです。
警備員による入場と身分証明書の確認が必要な、施錠された建物内。
近接バッジと指紋スキャナーでアクセスできるロックされたデータセンター内。
鍵のかかったキャビネット内では、警備員が最高情報セキュリティ責任者 (CISO) に電話して鍵を提供する許可を得る必要があります。
この機器のセキュリティをさらに強化するために、建築家が推奨すべき追加対策は次のどれですか?
A. データセンターにアクセスできるすべてのエンジニアに作業明細書に署名してもらいます。
B. キャビネットに焦点を当てたカメラを備えたビデオ監視システムを設置します。
C. このキャビネット内で作業を行う必要があるネットワーク エンジニアには、CISO が同行します。

D. いかなる理由であれデータセンターに入るすべての人に身元調査を受けることを義務付けます。
Answer: (解答を表示する**)**
キャビネットでのすべてのアクティビティを記録および監視することで、リアルタイムの抑止力、誰がいつアクセスしたかの監査証跡、インシデント発生時の法医学的証拠が提供され、セキュリティが大幅に強化されます。

最新問題**: 53**
ある組織はオンプレミスのデータセンターに一元的なログ記録機能を備えており、展開されたクラウドワークロードからのログ記録を統合できるソリューションを求めています。また、検出とアラートのメカニズムを自動化したいと考えています。以下のどれが要件を満たすのに最も適していますか？
A. IDS/IPS
B. SIEM
C. データレイク
D. Syslog
Answer: B (メーッセージを残す**)**
セキュリティ情報およびイベント管理システムは、オンプレミスおよびクラウド ソースからログを取り込んで正規化し、検出のための自動相関ルールを適用してアラートを発行し、集中ログ記録、分析、自動通知のニーズに正確に対応します。

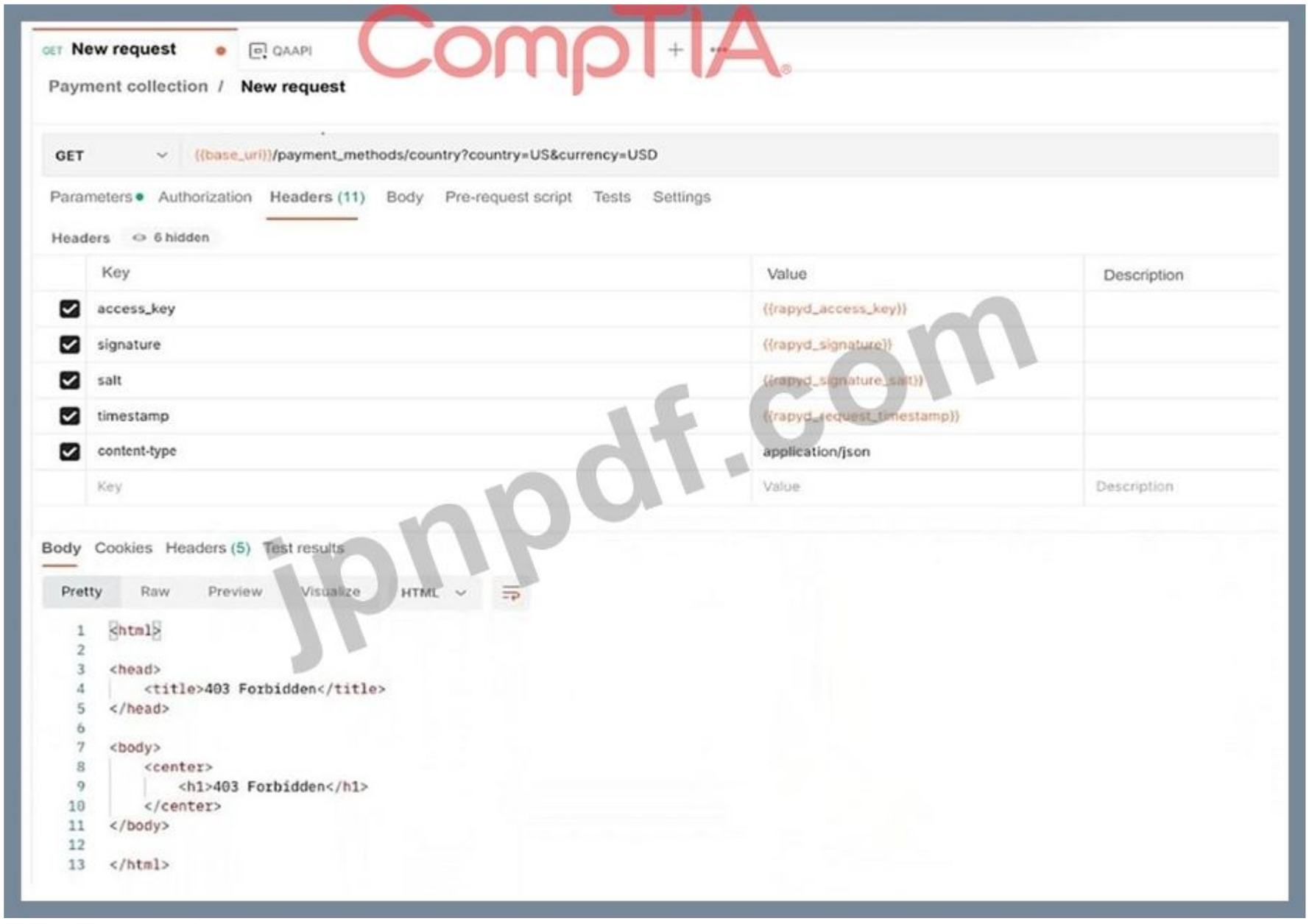
最新問題**: 54**
ネットワークセキュリティエンジニアは、パブリッククラウド内の仮想マシン上で実行されているウェブアプリケーションのセキュリティを確保する必要があります。仮想マシンはアプリケーションロードバランサーの背後に配置されています。エンジニアは、仮想マシンのセキュリティを確保するために、以下のどのテクノロジーを使用すべきでしょうか？ 2つ選択してください。）
A. CDN
B. DLP
C. IDS
D. WAF
E. 見る
F. NSG
Answer: D,F (メーッセージを残す**)**
WAF: ロード バランサーで受信 HTTP/HTTPS 要求を検査し、SQL インジェクション、XSS、その他の一般的な Web 攻撃をブロックすることで、Web アプリケーションを保護します。
NSG: VM のサブネットまたはインターフェースにネットワーク層の制御を適用し、承認されたポートと IP 範囲のみがアプリケーション サーバーにアクセスできるようにします。

最新問題**: 55**
ネットワーク セキュリティ管理者は、次のソリューションを設定する必要があります。
ログ ファイルからすべてのデータを 1 つの場所に収集します。
データを相関させてアラートを生成します。
管理者は次のどれを実装する必要がありますか?
A. Syslog
B. イベントログ監視
C. ログ管理

D. 見る
Answer: D (メーッセージを残す**)**
セキュリティ情報およびイベント管理システムは、さまざまなソースからのログ収集を一元化し、相関ルールを適用して実用的なアラートを生成します。

最新問題**: 56**
あるカフェではタブレット端末を使ったPOSシステムを導入しています。お客様から、料理の提供に時間がかかりすぎるという苦情が寄せられています。調査の結果、以下の点が判明しました。
すべてのキッチンプリンターが注文を印刷したわけではありません。
支払いは正常に処理されています。
クラウドベースのシステムには注文の記録が保存されます。
この問題はカフェが混雑していたときに発生しました。
この問題を軽減するための最善の方法は次のどれですか?
A. アプリケーションの更新
B. キッチン専用のアクセスポイントの追加
C. キッチンプリンターのワイヤレスドングルのアップグレード
D. キッチンプリンターに静的IPアドレスを割り当てる
Answer: B (メーッセージを残す**)**
プリンター専用のWi-Fiアクセスポイントを設けることで、プリンターのトラフィックを顧客向けタブレットから分離できます。これにより、混雑時の混雑を防ぎ、メインネットワークの負荷が高い場合でも注文を確実に印刷できます。

最新問題**: 57**
開発者がWebアプリケーションにアクセスしようとした際にエラーが発生したと報告しました。開発者はPostmanを使用してトラブルシューティングを行い、以下のエラーを受け取りました。



問題の原因は次のどれですか?

A. 要求された要素が見つかりません

B. ユーザー認証の欠如

C. NGFWルールが厳しすぎる

D. HTTPリダイレクトが正しくありません

Answer: (解答を表示する**)**

403 Forbidden HTMLレスポンスは、APIが呼び出しを拒否した原因が、リソース不足（404）、ネットワークレベルのブロック（タイムアウトまたはTCP拒否）、HTTPリダイレクトではなく、認証情報がない、または無効な認証情報（有効なアクセスキー/署名がない）であることを示します。403エラーを回避するには、有効な署名を持つ適切な認証ヘッダーが必要です。

最新問題**: 58**

ある組織の最高技術責任者（CTO）は、IaC を使用したネットワークの変更によって予定外の障害が発生することを懸念しています。このリスクを最も効果的に軽減できる方法は次のうちどれですか。

A. マスターブランチにコード変更を加える

B. 作者による変更のコードレビューの実施
C. 変更を加える前にコードリポジトリをフォークする
D. CI/CD パイプラインにレビュー/承認ステップを追加する
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
Infrastructure as Code（IaC）の変更による予定外の停止を防ぐ最善の方法は、CI/CDパイプラインに自動化されたレビューと承認ゲートを実装することです。これにより、すべての変更はデプロイ前に検証、ピアレビュー、テスト、そして場合によっては関係者による承認を受けることができ、本番環境に影響を与える問題の発生リスクを軽減できます。
CompTIA CloudNetX CNX-001 学習ガイドの「CI/CD セキュリティと IaC コントロール」の関連抜粋:
「CI/CDパイプラインに承認ゲートと自動検証を組み込むことで、デプロイメント前に構成ミスや不正な変更を検出し、停止のリスクを軽減できます。」その他のオプション：
* A. マスター ブランチに直接変更を加えることはベスト プラクティスに違反します。
* B. 自己レビュー（著者による）は客観性に欠け、同僚による検証に失敗します。
* C. フォークするとコピーが作成されますが、正式な検証プロセスは導入されません。