Fortinet.NSE5_SSE_AD-7.6.v2026-11-04.q48

試験コード：	NSE5_SSE_AD-7.6
試験名称：	Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator
認証ベンダー：	Fortinet
無料問題の数：	48
バージョン：	v2026-11-04
ページの閲覧量：	109
問題集の閲覧量：	567

https://www.jpnshiken.com/shiken/Fortinet.NSE5_SSE_AD-7.6.v2026-11-04.q48.html

質問: **1**
FortiGateデバイスが稼働中です。WANリンクの使用効率を最適化し、冗長性を向上させるため、SD-WANを有効化して設定します。
この構成更新プロセスの一環として、あなたは何をしなければなりませんか？
A. ファイアウォール ポリシーで SD-WAN メンバーとして使用されているインターフェイスへの参照を置き換えます。
B. ルーティング設定でSD-WANメンバーとして使用されているインターフェースへの参照を置き換えます。
C. SD-WANメンバーとして使用したいインターフェースを無効にします。
D. SD-WANライセンスを購入してインストールし、FortiGateデバイスを再起動します。
正解: **(**正解を表示します**)**
FortiGateでSD-WANを有効にすると、SD-WANゾーンに追加した個々のWANインターフェイスは、ファイアウォールポリシーで直接参照されなくなります。
その代わりに、ファイアウォールポリシーを更新して、SD-WANゾーンをインターフェースの参照として使用するようにする必要があります。

質問: **2**
FortiSASEの活用事例として考えられるのはどれですか？ 3つ選択してください）
A. セキュアインターネットアクセス(SIA)
B. セキュアSaaSアクセス SSA）
C. セキュアプライベートアクセス SPA）
D. セキュアVPNアクセス SVA）
E. セキュアブラウザアクセス (SBA)
正解: **A,B,C (**コメントを発表する**)**
FortiSASEは、3つの主要なセキュアアクセス利用事例を中心に設計されています。
セキュアインターネットアクセス SIA）
SWG、FWaaS、DNSセキュリティ、および脅威対策を使用して、ユーザーが公共インターネットにアクセスする際に保護します。
セキュアSaaSアクセス SSA）
可視性、制御性、データ保護機能を備え、クラウド／SaaSアプリケーションへのアクセスを安全に確保します。
セキュアプライベートアクセス SPA）
従来のVPNに公開することなく、プライベートアプリケーションへのゼロトラストアクセス ZTNA）を提供します。

質問: **3**
FortiGateにSD-WANルールを使用してローカルから外部へのトラフィックを制御させたい。

考慮すべき制約条件はどれですか？ (2つ選択してください。)
A. デフォルトでは、FortiGate は ping および traceroute に対応するローカルアウト トラフィックに対してのみ SD-WAN ルールを使用します。
B. デフォルトでは、ローカルアウトトラフィックはSD-WANを使用しません。
C. 手動戦略を使用する SD-WAN ルールでのみ、ローカルから送信へのトラフィックを制御できます。
D. SD-WANを使用するには、各ローカルアウト機能を個別に設定する必要があります。
正解: **(**正解を表示します**)**
デフォルトでは、ローカルアウトトラフィックはSD-WANを使用しません。→ FortiGateは通常、SD-WANルールを適用せずに、ローカルアウトトラフィック (DNS、NTP、FortiGuardアップデートなど) をインターフェース経由で直接送信します。
SD-WANを使用するには、各ローカル出力機能を個別に設定する必要があります → SD-WAN経由でローカル出力トラフィックをルーティングするには、SD-WANルールを使用するように、目的のローカル出力機能 (DNS、FortiGuard、CAPWAPなど) を明示的に設定する必要があります。

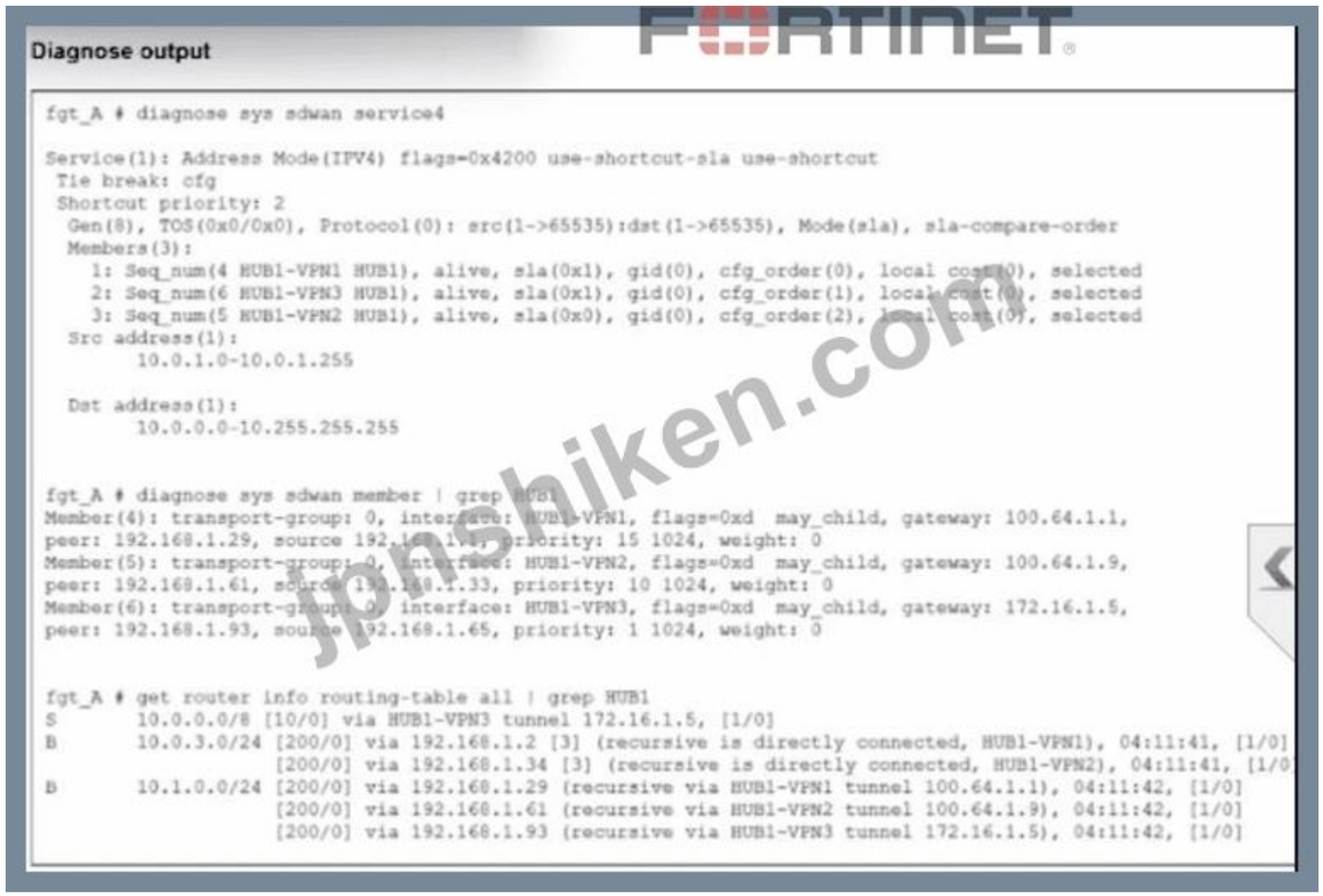
質問: **4**
展示資料を参照してください。



FortiSASEの脆弱性サマリーダッシュボードに関する記述のうち、正しいものはどれですか？ (2つ選択してください。)
A. ダッシュボードには、未知のアプリケーションの脆弱性スコアが表示されます。
B. エンドポイントプロファイルで脆弱性スキャンが無効になっています。
C. ダッシュボードを使用すると、管理者はドリルダウンして CVE データと深刻度分類を表示できます。
D. サポートされているアプリケーションでは、脆弱性の自動パッチ適用を有効にできます。
正解: **(**正解を表示します**)**
FortiSASE 7.6 およびそれ以降の2025バージョン) のカリキュラムと管理ガイドに基づくと、脆弱性サマリーダッシュボードはエンドポイントセキュリティ態勢管理の重要な構成要素です。
* ドリルダウン機能 (オプション C) FortiSASE 管理ガイドによると、セキュリティ ダッシュボードの脆弱性概要ウィジェットは対話型です。管理者は、特定のリスク カテゴリ (例：重大/高) またはアプリケーション タイプ (例オペレーティングシステム、Web クライアント) をクリックしてドリルダウンできます。この操作により、影響を受ける特定のエンドポイント、関連する CVE 識別子、および CVSS 標準に基づく深刻度分類を示す詳細ペインが開きます。
* 自動脆弱性パッチ適用 (オプション D): FortiSASE 7.6/2025 機能セットでは、エンドポイント プロファイル構成 (エンドポイント > 構成 > プロファイル) に「自動パッチ適用」が含まれています。

この機能により、脆弱性が検出された際に、サポートされているサードパーティ製アプリケーションおよび基盤となるオペレーティングシステム（Windows/macOS）のセキュリティ更新プログラムをシステムが自動的にインストールできます。さらに、管理者は脆弱性概要ウィジェットから特定の脆弱性を選択することで、これらのパッチの適用スケジュールを直接設定できます。
他の選択肢が間違っている理由：
* オプションA :ダッシュボードのカテゴリ（オペレーティングシステム、Webクライアント、Microsoft Officeなど）は、既知のソフトウェアシグネチャに基づいています。「その他」カテゴリもありますが、ダッシュボードは主にCVEデータが利用可能な既知のアプリケーションのスコアを提供します。
* オプションB :この図にはアクティブなデータ（合計57件の脆弱性）が表示されており、脆弱性スキャンが有効になっていて、現在エンドポイントからデータが報告されていることを示しています。無効になっている場合は、ウィジェットは空になるか、ゼロが表示されます。

質問: **5**



管理者がFortiGateのSD-WANのトラブルシューティングを行っています。branch1_fgtの背後にあるデバイスが10.0.0.0/8ネットワーク宛てのトラフィックを生成します。管理者は、このトラフィックがSD-WANルールID 1に一致し、HUB1-VPN1経由でルーティングされることを期待しています。しかし、実際にはトラフィックはHUB1-VPN3経由でルーティングされています。
展示されている出力結果に基づくと、観察された挙動を説明できる理由は、単独または組み合わせて、次のうちどれでしょうか？（2つ選択してください。）
A. HUB1-VPN1 には宛先への有効なルートがありません。
B. HUB1-VPN3 は HUB1-VPN1 よりも高いメンバー構成優先度を持っています。
C. HUB1-VPN3 は、HUB1-VPN1 よりもルート優先度値が低い (優先度が高い)。
D. トラフィックは、送信デバイスとして HUB1-VPN3 が設定された通常のポリシー ルートに一致します。

正解: **(**正解を表示します**)**
SD-WAN 7.6 コア管理者向けカリキュラムおよび図に示されている診断出力によると、トラフィックが期待される HUB1-VPN1 (SD-WAN ルール ID 1 で定義) ではなく HUB1-VPN3 にルーティングされる理由は、FortiOS の 2 つのコアルーティング原則によって説明できます。
* 有効なルート要件 (オプション A): 診断システム SDWAN サービス 4 の出力 (ルール ID 1 に対応) には、ルールに HUB1-VPN1、HUB1-VPN2、および HUB1-VPN3 のメンバーがあることが示されています。SD-WAN ステアリングの重要な原則は、メンバーがルールによって 「選択可能」になるには、ルーティング テーブル (RIB/FIB) に宛先への有効なルートがなければならないということです。ルーティング テーブルの出力 (図の 3 番目のセクション) に、HUB1-VPN3 経由の 10.0.0.0/8 へのルートが表示されていても、HUB1-VPN1 経由のルートが表示されていない場合、SD-WAN エンジンは、その特定の宛先に対して HUB1-VPN1 が 「到達不可能」なパスとみなされるため、HUB1-VPN1 を完全にスキップします。
* ポリシー ルートの優先順位 (オプション D): FortiOS のルート検索階層では、通常のポリシー ルート (PBR) が SD-WAN ルールよりも先に評価されます。管理者が、10.0.0.0/8 宛てのトラフィックに一致し、送信インターフェイスとして HUB1-VPN3 を指定する従来のポリシー ルート ([ネットワーク] > [ポリシー ルート] にあります) を設定している場合、FortiGate はそのポリシー ルートに基づいてパケットを転送し、そのセッションの SD-WAN ルールは評価しません。この 「バイパス」は、SD-WAN ルールが 「より良い」リンクを選択するかどうかに関係なく発生します。
他の選択肢が間違っている理由：
* オプション B: メンバー構成の優先順位 (cfg_order) は一部の戦略ではタイブレーカーとなりますが、SD-WAN ルールロジックは、ルーティングテーブルがそれを許可する場合、または優先順位の高いポリシー ルートが最初にトラフィックをインターセプトしない場合にのみ適用されます。
* オプション C: ルート優先度が低い（つまり、RIB での優先度が高い）場合 暗黙のルール（標準ルーティング）に影響します。ただし、SD-WAN ルールは、一致するトラフィックに対して RIB 優先度を上書きするように設計されています。
HUB1-VPN1が有効な候補であり、かつポリシールートが存在しない場合、SD-WANルールは通常、RIBの優先順位を無視して独自のルーティング戦略を適用します。

質問: **6**
FortiSASEでは、ジオフェンシング機能はどのように使用されますか？（回答は1つ選択してください）
A. 特定の国にあるモバイルデバイス上の保存データを暗号化する。
B. 特定の国において、時間帯に基づいてアプリケーションへのアクセスを制限する。
C. 特定の国からのFortiSASE POPへのリモートユーザー接続を許可またはブロックします。
D. ウェブサイト上でのユーザー行動を監視し、特定の国からの業務に関係のないコンテンツをブロックする。
正解: **C (**コメントを発表する**)**

質問: **7**
トラフィックが暗黙のSD-WANルールに一致した場合に何が起こるかを正しく説明しているのは、次のうちどれですか？（2つ選択してください。）
A. トラフィックは、v4-ecmp-mode 設定で設定されたアルゴリズムを使用して負荷分散されます。
B. トラフィックがポリシー経路テーブルのエントリのいずれにも一致しません。
C. FortiGate はセッションに may_dirty と vwl_default のフラグを付けます。
D. トラフィックは、重量に関係なく、利用可能なすべての静的ルートに分散されます。
E. セッション情報出力にSD-WANサービスIDが表示されません。
正解: **(**正解を表示します**)**
トラフィックが暗黙のSD-WANルールに一致する場合、セッションにはmay_dirtyとvwl_defaultのフラグが付けられ、デフォルトのSD-WAN動作によって処理されたことが示されます。
暗黙のルールが使用されるため、特定のSD-WANサービスが一致せず、セッション情報にはSD-WANサービスIDが表示されません。

質問: **8**

展示資料を参照してください。

FortiGate router policy and diagnose output

```
branch1_fgt # show router policy
config router policy
    edit 1
        set src "10.0.1.128/255.255.255.128"
        set dst "128.66.0.0/255.255.255.0"
        set action deny
    next
end

branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), Health-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.769, selected
    2: Seq_num(1 port1 underlay), alive, latency: 71.022, selected
  Application Control(3): Microsoft.Portal(41469,0) Salesforce(16920,0) Collaboration(0,28)
  Src address(1):
        10.0.1.0-10.0.1.255

Service(4): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(2):
    1: Seq_num(1 port1 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(2 port2 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        128.66.0.0-128.66.255.255
```

FortiGateは、送信元IPアドレスが10.0.1 130、宛先IPアドレスが128 66.0 125のトラフィックをどのように処理しますか？

A. FortiGateはポート2を介してトラフィックの流れを制御します

B. FortiGateがトラフィックフローをドロップします

C. FortiGateはFIBに従ってトラフィックフローをルーティングします。

D. FortiGateはポート1とポート2を介したトラフィックフローを負荷分散します

正解: **C** (コメントを発表する)

正解はCです。FortiGateはFIBに従ってトラフィックフローをルーティングします。図は、送信元10.0.1.128/255.255.255.128、宛先128.66.0.0/255で構成された通常のポリシー ルートを示しています。

255.255.0。テスト送信元10.0.1.130は10.0.1.128/25サブネットに属し、宛先128.66.0.125は128.66.0.0/24に属しているため、このトラフィックはこのポリシー ルートに一致します。

FORTINET
jpnshiken.com

重要な点として、このルートには「拒否」アクションが設定されています。ルーターポリシーの場合、これはファイアウォールの「拒否」のようにFortiGateがパケットを破棄することを意味するものではありません。これは「ポリシールーティングの停止」を表します。Fortinetは、パケットがこのアクションに一致すると、FortiGateはポリシールーティング処理を停止し、転送情報ベース（FIB）を使用してパケットをルーティングすると説明しています。
通常のポリシー ルートは、SD-WAN ルールよりも優先されます。したがって、図に示す SD-WAN サービス 4 は、送信元 10.0.1.0～10.0.1.255、宛先 128.66.0.0～128.66.255.255 に一致しますが、ポート 1 とポート 2 のラウンド ロビン選択はこのフローを制御しません。一致する通常のポリシー ルートが、ポリシー ルーティングを先に終了します。
学習ガイド参照：SD-WAN構成と監視 > ポリシールート > ルート検索とFIB処理、423～424ページ。

質問: **9**
FortiSASEのリモートユーザーに対する安全な本人確認とアクセス制御をサポートする認証ソースはどれですか？（3つ選択してください。）
A. リモート認証ダイヤルインユーザーサービス (RADIUS)
B. OpenID Conned (OIDC)
C. 端末アクセスコントローラ・アクセス制御システムプラス（TACACS+）
D. セキュリティアサーションマークアップ言語（SAML）
E. 軽量ディレクトリアクセスプロトコル（LDAP）
正解: **(**正解を表示します**)**

質問: **10**
エージェントレスZTNAを動作させるために必要な設定はどれですか？（2つ選択してください。）
A. プロキシユーザーによるシングルサインオン（SSO）
B. FortiClientエージェント
C. ZTNAプロキシを搭載したFortiGate
D. SD-WANプライベートアクセスSPA
正解: **(**正解を表示します**)**
エージェントレスZTNAでは、ZTNAプロキシとして機能するFortiGateが必要であり、FortiClientエージェントを必要とせずにユーザーを識別するためにプロキシベースのシングルサインオン（SSO）に依存します。

質問: **11**
トラフィックが暗黙のSD-WANルールに一致した場合に何が起こるかを正しく説明しているのは、次のうちどの2つの記述ですか？
（2つ選択してください）
A. トラフィックは、v4-ecmp-mode 設定で設定されたアルゴリズムを使用して負荷分散されます。
B. トラフィックがポリシー経路テーブルのエントリのいずれにも一致しません。
C. FortiGate はセッションに may_dirty と vwl_default のフラグを付けます。
D. トラフィックは、重量に関係なく、利用可能なすべての静的ルートに分散されます。
E. セッション情報出力にSD-WANサービスIDが表示されません。
正解: **(**正解を表示します**)**
SD-WAN 7.6 Core Administrator 学習ガイドおよび FortiOS 7.6 管理ガイドによると、「暗黙のルール」は SD-WAN ルールリストの一番下にあるデフォルトルール (ID 0) です。このルールは、トラフィックが手動で設定された SD-WAN ルールに一致しない場合にのみ評価されます。

ポリシールーティングテーブルのコンテキスト（オプションB）SD-WANルールは、技術的にはポリシーベースルーティングの特殊な形式です。パケットが暗黙のルールに一致するには、まずルーティング階層を通過する必要があります。トラフィックが暗黙のルールに一致する場合、それは、トラフィックを以前に遮断するはずだった、より優先度の高いユーザー定義のSD-WANルールや、手動ポリシールーティングテーブルの特定のエントリに一致しなかったことを示します。
セッション情報（オプション E）CLI を使用してアクティブなセッションを検査する場合（例diagnose sys session list）、出力には SD-WAN サービス ID のフィールドが含まれます。トラフィックがユーザー定義ルールによってルーティングされている場合、そのルールの ID が表示されます（例service_id=1）。ただし、トラフィックが暗黙のルールにフォールスルーする場合、セッション情報には SD-WAN サービス ID は表示されません（多くの場合 0 と表示されるか、省略されます）。これは、暗黙のルールがユーザー定義ルールと同じように「サービス」として機能しないためです。
ルーティング動作：暗黙のルールは、標準ルーティングテーブル（RIB/FIB）のロジックに従います。静的ルートの優先度と距離を使用してパスを決定します。複数のパスが同じ距離と優先度を持つ場合、v4-ecmp-modeで設定されたアルゴリズムを使用しますが、これはルーティングエンジンの機能であり、SD-WANエンジン自体の機能ではありません。
他の選択肢が間違っている理由：
オプションA :v4-ecmp-mode（例ソースIPベース）はECMPルーティングに使用されますが、これはFIB内の等コストパスに対する一般的なFortiOSルーティング動作の一部であり、暗黙のルールは単にそのルーティングテーブルに決定を「委ねる」だけです。
オプション C: トラフィックが暗黙のルールに一致すると、セッションは実際には vwl_id=0 でフラグ付けされ、ルート変更が発生した場合はダーティになる可能性がありますが、vwl_default はカリキュラムのこの特定のコンテキストで使用される標準のフラグ名ではありません。
選択肢D :これは誤りです。暗黙のルールは、ルーティングテーブル内の静的ルートで定義されている重み、距離、優先度を尊重します。これらの値に関係なくトラフィックを分散するわけではありません。

質問: 12

図を参照してください。FortiGateデバイスのSD-WANイベントログ2件、メンバーの状態、SD-WANルールの設定、およびヘルスチェックの設定が示されています。
ログメッセージが表示された直後、FortiGateは図に示された情報に基づいてどのようにトラフィックを制御しますか？（回答を1つ選択してください）

SD-WAN event logs



Identity

Device ID	FGVM02TM25002088
Device Name	branch1_fgt

Type

Sub Type	sdwan
Type	event

Alerts

Action	
Level	notice

General

Log Description	SDWAN status
Log ID	0113022923
Member	1
Message	Member status changed. Member out-of-sla.
Virtual Domain	root

Others

Date	2025-07-01
Date/Time	2025-07-01 05:00:25
Destination End User ID	3
Destination Endpoint ID	3
Destination Geo ID	0
Device Time	2025-07-01 05:00:25
Device Time Zone	-0700
Event Time	2025-07-01 05:00:25
Event Type	Health Check
Health Check	Corp_HC
Log Flag	0
SLA Target ID	1
Source City	Sunnyvale

```
config service
    edit 1
        set name "Critical-DIA"
        set mode sla
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16920 41469
        set internet-service-app-ctrl-category 28
        config sla
            edit "Corp_HC"
                set id 1
            next
        end
        set priority-members 1 2
    next
```

SD-WAN health-check configuration

```
branch1_fgt (health-check) # show
config health-check
    edit "Corp_HC"
        set server "198.18.1.1" "198.18.1.2"
        set member 1 2
        config sla
            edit 1
                set latency-threshold 150
                set jitter-threshold 50
                set packetloss-threshold 5
            next
        end
    end
```



Identity

Device ID	FGVM02TM25002088
Device Name	branch1_fgt

Type

Sub Type	sdwan
Type	event

Alerts

Action	
Level	notice

General

Log Description	SDWAN status
Log ID	0113022923
Message	Number of pass member changed.
Virtual Domain	root

Others

Date	2025-07-01
Date/Time	2025-07-01 05:00:25
Destination End User ID	3
Destination Endpoint ID	3
Destination Geo ID	0
Device Time	2025-07-01 05:00:25
Device Time Zone	-0700
Event Time	2025-07-01 05:00:25
Event Type	Health Check
Health Check	Corp_HC
Log Flag	0
New Value	1
Old Value	2

jpnshiken.com

A. FortiGateはポート1またはポート2を使用してSD-WANルールID 1のトラフィックをルーティングします。
B. FortiGateはポート1を使用してSD-WANルールID 1のトラフィックをルーティングします。
C. FortiGateはポート2を使用してSD-WANルールID 1のトラフィックをルーティングします。
D. FortiGate は SD-WAN ルール ID 1 をスキップします。
正解: **C** (コメントを発表する)
SD-WAN 7.6コア管理者向けカリキュラムおよび提供されている資料によると、トラフィックのルーティング決定は、最低コスト（SLA）戦略とイベントログに報告されるリンクの健全性ステータスとの相互作用によって決定されます。
ルール戦略（最低コストSLA）ID 1（Critical-DIAという名前）のSD-WANルール設定は、slaモードに設定されています。このモードでは、FortiGateは割り当てられたパフォーマンスSLA目標を満たすメンバーインターフェイスのみを介してトラフィックをルーティングします。
メンバーの優先順位: このルールでは、priority-members 1 2 と定義されています。これは、通常の状態（両方のリンクが正常な状態）では、メンバー 1（ポート 1）が最初にリストされているため、優先インターフェースとなることを意味します。
イベントログ分析:
最初のログメッセージには、メンバーに対して「メンバーのステータスが変更されました。メンバーがSLA外です。」と明示的に記載されています。
1. これは、ポート1がCorp_HCヘルスチェックで定義されているしきい値（遅延、ジッター、またはパケット損失）のいずれかを超えたことを示しています。
2 番目のログには「パス メンバー数が変更されました。新しい値: 1、古い値: 2」と記載されています。これは、以前は 2 つのリンクが SLA をパスしていたのに対し、現在は 1 つのリンク (メンバー 1、2、3、4、5、6、7、8、9、1、1、3、1、2、3、1、4、5、6、7、8、9、1、2、1、2、3、1、2、2、3、2、4、2、3、4、5、2/ポート2)は通過状態のままです。

ステアリング決定 :ルール戦略がSLAモードであり、優先メンバー ポート1)がSLAを満たしていないため、FortiGateは直ちにメンバー1をこの特定のルールの選択プールから除外します。その後、優先順位リスト内でSLAを満たす次の利用可能なメンバーであるメンバー2 ポート2)に移動します。

質問: **13**
図を参照してください。この図は、FortiGate デバイスで取得したコマンド「diagnose sys sdwan service」の出力結果を示しています。
管理者は、FortiGateがサブネット10.0.1.0/255.255.255.192上のローカルユーザーからのトラフィックを、ソーシャルメディアアプリケーションFacebook宛てにどのインターフェース経由でルーティングするかを知りたいと考えています。
展示物に基づいて、正しい記述は次のうちどれですか？ 2つ選択してください。)

```
fgt_1 # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-
threshold(10), heath-check(HQ_Servers)

   Members(2):
     1: Seq_num(1 port1), alive, latency: 2.672, selected
     2: Seq_num(2 port2), alive, latency: 2.570, selected
   Internet Service(2): Facebook(4294836714,0,0,0,0 15832) Twitter(4294838045,0,0,0,0 16001)
   Src address(1):
         10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
   Members(1):
    1: Seq_num(2 port2), alive, selected
   Internet Service(2): Business(0,29,0,0,0) Industrial(0,26,0,0,0)
   Src address(1):
         10.0.1.0-10.0.1.255

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
   Members(3):
     1: Seq_num(3 T_HQ1), alive, alive, sla(0x3), gid(0), cfg_order(0), local cost(0), selected
     2: Seq_num(4 T_HQ2), alive, alive, sla(0x2), gid(0), cfg_order(1), local cost(0), selected
     3: Seq_num(5 T_HQ3), alive, alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
   Src address(1):
         10.0.1.0-10.0.1.255
   Dst address(1):
         10.0.0.0-10.255.255.255
```

jpnshiken.com
FORTINET®

A. FortiGateは、サービスルール2に従ってソーシャルメディアアプリケーションのトラフィックをルーティングし、ポート2を介してトラフィックをルーティングします。
B. Facebook アプリケーションにはサービスが定義されていないため、FortiGate はサービス ルール 3 を適用し、トラフィックを本社に転送します。

C. FortiGateがフローのアプリケーションを認識できない場合、HQ_T1、HQ_T2、HQ_T3トンネルを介してトラフィックを負荷分散します。
D. FortiGate がフローのアプリケーションを認識できない場合、ルール 3 の優先メンバーである HQ_T1 を介してトラフィックをルーティングします。
正解: **(**正解を表示します**)**
フローが定義済みのアプリケーションカテゴリ（ソーシャルメディアなど）に属すると識別された場合、FortiGateはそれを対応するサービスルール（ルール2）に照合し、ポート2などの指定されたインターフェース経由でルーティングします。ただし、セッション設定中にアプリケーションが認識されない場合、システムはデフォルトで、未分類トラフィックのポリシーに従って利用可能なトンネルを使用してトラフィックの負荷分散を行い、アプリケーションの分類を待っている間も継続的な接続を確保します。」これにより、パフォーマンスと耐障害性の両方が保証されます。

質問: **14**
FortiSASEのCASB機能に関する記述として正しいのはどれですか？
A. FortiSASEは、APIベースのCASBとインラインCASBの両方を提供します。
B. FortiSASEはAPIベースのCASBのみを提供します
C. FortiSASEはインラインCASBのみを提供します
D. FortiSASEは、セキュリティファブリックとの統合を通じてのみCASB機能を提供します。
正解: **(**正解を表示します**)**
正解はAです。FortiSASEは、APIベースのCASBとインラインCASBの両方を提供します。Fortinetは、FortiSASE Secure SaaS Accessが、インライン検査と帯域外のAPIベースの検査を組み合わせたデュアルモードCASBアーキテクチャを採用していると説明しています。これにより、SaaSの使用状況を可視化および制御できるだけでなく、転送中のデータと保存中のデータの両方を保護できます。
インラインCASBは、エンドポイントとSaaSアプリケーション間のトラフィックパスで直接動作します。FortiSASEは、アプリケーション制御、Webフィルタリング、SSLディープインスペクション、DLPなどの機能を使用して、アプリケーションを識別し、SaaSアクセス制御を適用し、トラフィックを検査し、転送中のデータを保護します。学習ガイドでは、インラインコンポーネントがSaaSアプリケーションのトラフィックを認識し、プロトコルデコーダとHTTPインスペクションを使用して制御を適用すると具体的に説明しています。
APIベースまたはアウトオブバンドCASBは、APIを介してサポートされているクラウドアプリケーションに直接接続します。その主な役割は、SaaSサービスに既に保存されている静止データを検査および評価することです。FortiSASE Enterpriseの資料でも同様に、FortiCASBはクラウド/APIベースの機能を提供すると同時に、FortiSASEはWebフィルタとアプリケーション制御を介してインラインCASBを提供すると明記されています。
したがって、BとCはFortiSASEを1つのCASBモードに限定するという誤った判断を下しており、Dはセキュリティファブリックの統合を前提条件とするという誤った判断を下している。
学習ガイド参照 :SIAおよびSSA > セキュアSaaSアクセス > インラインCASBおよびアウトオブバンドCASB、ページ
105-108。

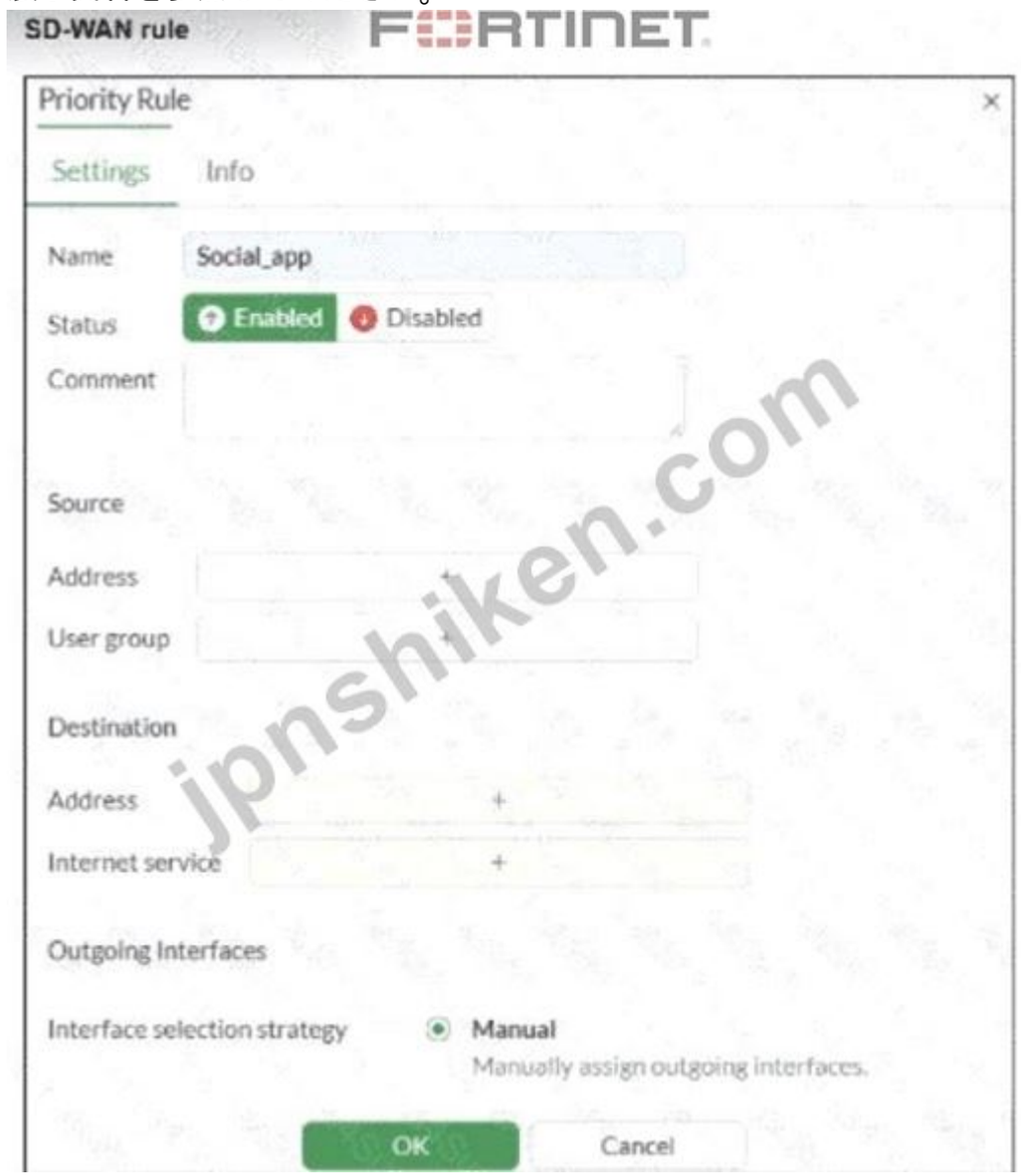
質問: **15**
FortiSASEがサポートする導入環境について、正しい記述はどれですか？
A. FortiSASEは、ユーザーの要件に基づいて、VPNモードとエージェントレスモードをサポートします。
B. FortiSASEは、展開状況に応じてエンドポイントモードとSWGモードの両方をサポートします。
C. FortiSASEはSWGモードでのみ動作し、すべてのトラフィックはFortiSASE POPを経由するように強制されます。
D. FortiSASEはZTNAのみのモードに依存しており、SWGとエンドポイント機能は置き換えられています。
正解: **(**正解を表示します**)**
FortiSASE 7.6 管理ガイドおよび FCP - FortiSASE 24/25 管理者カリキュラムによると、FortiSASE はさまざまなユーザーおよびデバイスの要件をサポートするためにハイブリッド展開アーキテクチャで設計されています。主に次の 2 つのモードで動作します。

* エンドポイントモード（エージェントベース）：このモードでは、ユーザーのラップトップまたはデバイスにFortiClientをインストールする必要があります。エージェントは、最寄りのFortiSASE Point of Presence（PoP）への常時接続のセキュアVPNトンネルを確立し、セキュアインターネットアクセス（SIA）、セキュアプライベートアクセス（SPA）、およびエンドポイントの姿勢チェック（ZTNA）を完全に提供します。
* セキュアWebゲートウェイ（SWG）モード（エージェントレス）：このモードは、エージェントのインストールが不可能なユーザーまたはデバイス（管理対象外デバイスやChromebookなど）に使用されます。明示的なWebプロキシ設定またはPAC（プロキシ自動構成）ファイルを使用して、Webトラフィック（HTTP/HTTPS）をSASE PoPにリダイレクトし、検査を行います。
他の選択肢が間違っている理由：
* オプション A: VPN をサポートしていますが、「VPN モード」はデプロイメント タイプの正式名称ではありません。「エンドポイントモード」
* オプション C: FortiSASE は SWG に限定されず、FWaaS および ZTNA を含む完全な SSE (Security Service Edge) ソリューションです。
* オプション D: ZTNA はプラットフォーム内の機能であり、エンドポイントまたは SWG 機能の全体的な代替ではありません。

質問: **16**
SD-WANルールを設定する際に、SLA目標とSD-WANルールに関して考慮すべき3つの要素は何ですか？（3つ選択してください）
A. SD-WANルールを設定する際、異なるパフォーマンスSLAから複数のSLAターゲットを選択できます。
B. SLAターゲットは、最低コスト（SLA）戦略で構成されたSD-WANルールでのみ使用されます。
C. メンバーの指標は、ルールがSLAターゲットを使用している場合にのみ測定されます。
D. SD-WANルールはSLAターゲットを使用して、優先メンバーがSLA要件を満たしているかどうかを確認できます。
E. SD-WANルールを設定する際、同じパフォーマンスSLAに属する複数のSLAターゲットを選択できます。
正解: **B,D,E** (コメントを発表する)
SD-WAN 7.6 Core Administrators学習ガイドおよびFortinetドキュメントライブラリによると、SD-WANルールとSLAターゲット間の相互作用は、特定の選択および測定ロジックによって制御されます。
* 戦略による使用（オプション B）：SLA ターゲットは、基本的に最低コスト（SLA）戦略によって使用され、トラフィック ステアリングの対象となるリンクが現在十分に健全であるかを判断します。ベスト クオリティなどの他の戦略では、メトリックを監視するために「測定済み SLA」を使用しますが、通常は SLA ターゲットを使用しません。
「必須SLA目標」は、ハイブリッドモードで明示的に設定されていない限り、リンクを無効にするためのものです。ほとんどのカリキュラムでは、「必須SLA目標」フィールドは、特に「最低コスト」および「帯域幅最大化」戦略に関連付けられています。
* SLA準拠チェック（オプションD）：SD-WANルールは、SLAターゲットを「合格／不合格」判定のゲートキーパーとして利用します。エンジンは、優先メンバーが定義されたSLA要件（遅延、ジッター、パケット損失のしきい値）を満たしているかどうかを確認します。優先メンバーがSLAを満たさない場合、ルールはSLAを満たす優先順位リストの次のメンバーに移動します。
* 単一SLAバインディング（オプションE）：SD-WANルールを設定する際、GUIとCLIでは複数のSLAターゲットを選択できますが、それらはすべて同じパフォーマンスSLAプロファイルに属している必要があります。単一のSD-WANルール内で、異なるヘルスチェックのターゲット（例：「Google_HC」のターゲット1と「Amazon_HC」のターゲット2）を混在させることはできません。
他の選択肢が間違っている理由：
* オプション A: これは誤りです。単一の SD-WAN ルールは、一度に 1 つの特定のパフォーマンス SLA プロファイルにのみ関連付けることができるため、異なる SLA からターゲットを選択することはできません。
* オプションC：これは誤りです。メンバーメトリック（レイテンシ、ジッター、パケット損失）は、SD-WANルールが現在そのSLAターゲットをステアリング決定に使用しているかどうかに関わらず、パフォーマンスSLAプローブによって測定されます。測定はヘルスチェックの機能であり、ルールマッチングプロセスの機能ではありません。

有効的な**NSE5_SSE_AD-7.6**問題集はJPNTest.com提供され、**NSE5_SSE_AD-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE5_SSE_AD-7.6**試験問題集を提供します。JPNTest.com NSE5_SSE_AD-7.6試験問題集はもう更新されました。ここで**NSE5_SSE_AD-7.6**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/NSE5_SSE_AD-7.6-mondaishu **50**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 17
展示資料を参照してください。



スタンドアロンのFortiGateデバイスでSD-WANを設定します。FacebookとLinkedInに関連するトラフィックを、よりコストの低いインターネット回線経由でルーティングするSD-WANルールを作成したいと考えています。GUIからFacebookとLinkedInアプリケーションを宛先として設定するには、どのような手順が必要ですか？

A. アプリケーションをSD-WANルールの宛先として許可するライセンスをインストールします。
B. インターネットサービス分野では、FacebookとLinkedInを選択してください。
C. スタンドアロンの FortiGate デバイスでは、アプリケーションを SD-WAN ルールの宛先として設定することはできません。

D. SD-WANルールの宛先としてアプリケーションフィールドの表示を有効にします。
正解: (正解を表示します)
SD-WAN 7.6 コア管理者カリキュラムおよび FortiOS 7.6 管理ガイドによると、
SD-WANルールでFacebookやLinkedInなどの一般的なWebベースのサービスを宛先として設定することは、主にインターネットサービスデータベース（ISDB）を通じて行われます。
* インターネットサービスとアプリケーション制御：FortiOSでは、インターネットサービス（既知のIPアドレスとポートのデータベースを使用して最初のパケットでトラフィックを識別する）とアプリケーション（IPSエンジンがパケットフローをさらに深く検査してレイヤー7シグネチャを識別する必要がある）が区別されています。
* SD-WANの効率性：Fortinetは、FacebookやLinkedInなどのサービスに対してSD-WANルールでインターネットサービスフィールドを使用することを推奨しています。これは、FortiGateが最初のパケットを受信した時点でトラフィックを即座にルーティングできるためです。代わりに「アプリケーション」シグネチャを使用した場合、最初のハンドシェイクが完了するまでアプリケーションが識別されないため、最初のセッションが誤ってルーティングされる可能性があります。
* GUI設定：図（image_b3a4c2.png）に示すように、SD-WANルールの「宛先」セクションには、デフォルトでインターネットサービスフィールドが含まれています。FacebookとLinkedInのトラフィックをルーティングするには、管理者はそのフィールドの「+」アイコンをクリックし、データベースからFacebookとLinkedInのエントリを選択するだけです。
* 機能の可視性（代替案）：[システム] > [機能の可視性]で特定の「アプリケーション」フィールドを有効にすることはできますが（「アプリケーション検出ベースのSD-WAN」を有効にする）、これは通常、専用のISDBエントリを持たないあまり一般的でないアプリケーションに使用されます。前述の特定の「アプリケーション」（FacebookとLinkedIn）は、インターネットサービスフィールドにネイティブに存在するため、オプションBが最も直接的で一般的な実装方法となります。
他の選択肢が間違っている理由：
* オプション A：アプリケーション署名のライセンスは標準の FortiGuard サービスの一部であり、SD-WAN ルールの「宛先としてのアプリケーション」にのみ固有の前提条件ではありません。
* オプション C：スタンドアロンの FortiGate デバイスは、SD-WAN ルールにおけるアプリケーションベースおよび ISDB ベースのステアリングを完全にサポートします。
* オプション D：機能の表示を有効にすると、L7 アプリケーションにフィールドが追加されますが、デフォルトの GUI レイアウトで提供されているインターネット サービス フィールドから既にアクセスできる Facebook と LinkedIn には「必須」ではありません。

質問: **18**
小規模なサイトの場合、管理者はSD-WANを導入し、業務上重要なアプリケーションの高いネットワーク可用性を確保すると同時に、全体的なコストと従量課金制のバックアップ接続のコストを抑えることを計画している。
この計画を達成するために、管理者はどのような行動をとらなければならないか？
A. ミッドレンジのFortiGateデバイスを使用して、スタンドアロンSD-WANを実装します。
B. 動的ルーティングを実装する。
C. スタンドアロンSD-WANを実装するために、高可用性（HA）クラスタをセットアップします。
D. 少なくとも2つのWANリンクを設定してください。
正解: (正解を表示します)
SD-WANでは、複数のWANリンクが必要となり、リンクの状態を監視してトラフィックを動的にルーティングすることで、業務上重要なアプリケーションの負荷分散、フェイルオーバー、高可用性を実現します。単一のWANリンクでは冗長性を提供できないため、効率的な利用によって従量課金制のバックアップコストを抑えるには、小規模サイトであってもデュアルリンクが不可欠です。

質問: **19**

展示資料を参照してください。



どのウェブフィルタカテゴリへのアクセスが拒否され、ユーザーに代替メッセージが表示されますか？

A. 薬物乱用

B. 差別

C. ハッキング

D. 違法または非倫理的

正解: **(**正解を表示します**)**

正解はA. 薬物乱用です。図では、FortiGuardウェブフィルタカテゴリ 薬物乱用」が ブロック」アクションで設定されています。FortiSASEは、要求されたWebサイトに割り当てられたFortiGuardカテゴリに従って、設定されたアクションを適用します。FortiSASE管理者学習ガイドでは、 ブロック」アクションは、設定されたカテゴリに属するURLへのアクセスを拒否し、代替メッセージを表示するアクションとして明確に定義されています。

表示されている他のカテゴリは、それぞれ異なる動作をします。ハッキングは 監視」に設定されており、トラフィックの処理は 許可」と同様ですが、一致するトラフィックが検出されるたびにログエントリが生成されます。そのため、ユーザーのアクセスは拒否されません。違法または非倫理的なトラフィックは 警告」に設定されており、警告ページが表示されますが、ユーザーが選択すれば続行できます。差別は 許可」に設定されているため、トラフィックは残りの検査エンジンを通過し、ブロックされません。

したがって、この展示では、要求された動作 アクセスを拒否し、代替メッセージを表示する）がブロックアクションに直接マッピングされており、薬物乱用は、そのように設定されている唯一のカテゴリです。

学習ガイド参照 :セキュリティとエンドポイントプロファイル > インラインCASBを使用したWebフィルタ > FortiGuardカテゴリフィルタ、118ページ。

質問: **20**

パフォーマンスSLAをプローブモード パッシブ優先」に設定しました。

この構成による目に見える影響を2つ挙げてください。 2つ選択してください。）

A. FortiGateは、受動監視の対象となるトラフィックをハードウェアにオフロードできます。

B. FortiGateは、ICMPトラフィックがメンバーを通過しているかどうかをパッシブに監視します。

C. パッシブモニタリング中は、SLAパフォーマンスルールではデッドメンバーを検出できません。

D. FortiGateがアクティブモードに切り替わった後、SLAパフォーマンスルールは3分後にパッシブ監視に戻ります。

E. FortiGateは、TCPトラフィックがメンバーを通過しているかどうかをパッシブに監視します。

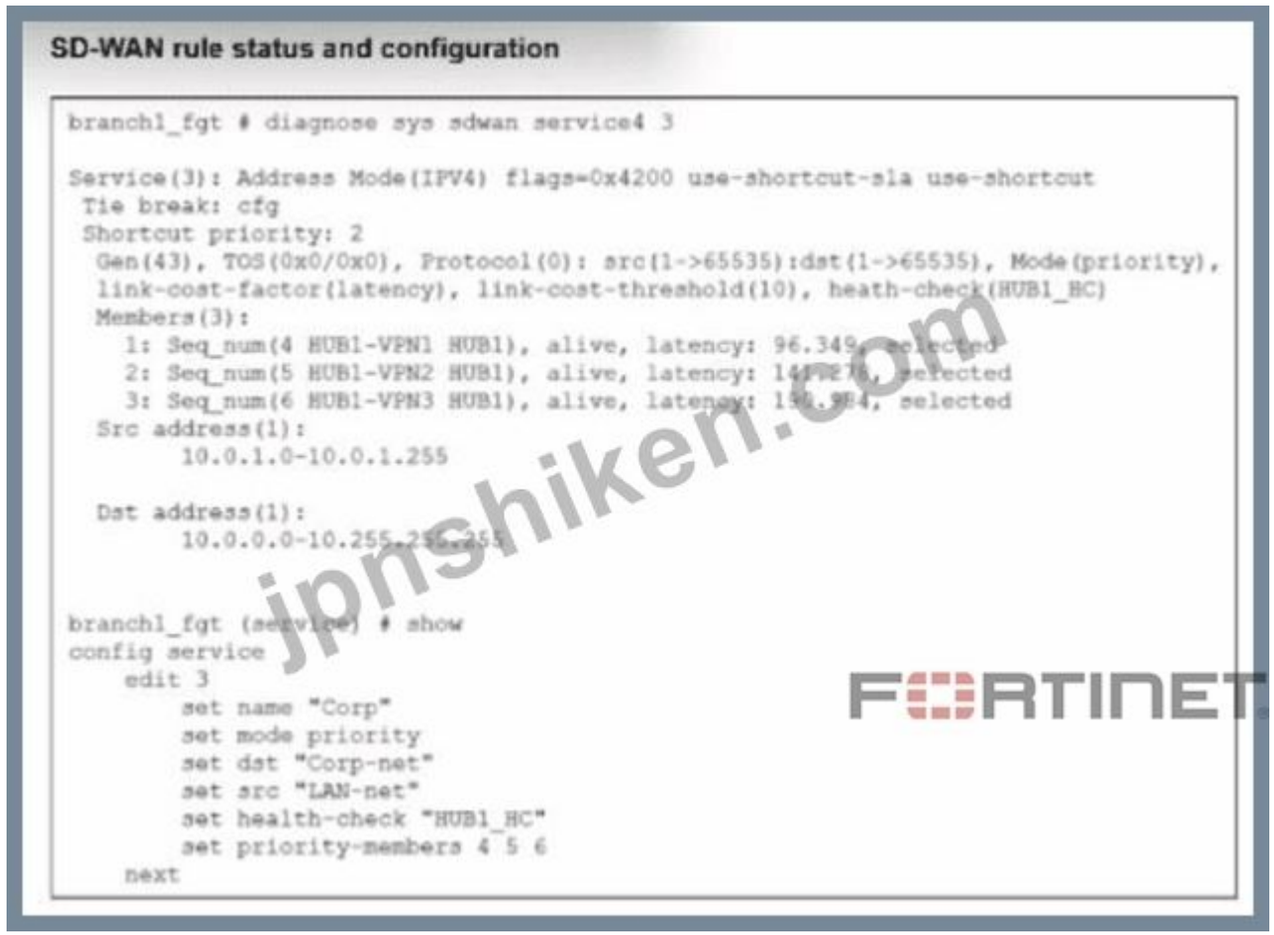
正解: **C,E (**コメントを発表する**)**

パッシブ優先」が設定されている場合、FortiGateはTCPセッションなどの実際のアプリケーショントラフィックを使用してSD-WANメンバーの状態をパッシブに監視し、実際に観測されたフローから遅延、ジッター、パケット損失などの統計情報を収集します。

パッシブ監視ではプローブパケットは生成されず、既存のトラフィックに完全に依存します。一致するトラフィックがない場合、ヘルスチェックデータは利用できないため、パッシブ監視のみが有効になっている場合、故障したメンバーが検出されない可能性があります。

質問: **21**
FortiSASEにおけるセキュリティ態勢タグに関する記述として正しいのはどれですか？
A. エンドポイントには複数のタグを割り当てることができますが、評価に使用されるのは1つだけです。
B. エンドポイントに複数のタグを割り当てて評価に使用できます。
C. タグは静的であり、エンドポイントの状態によって変更されません。
D. エンドポイントにはタグを1つだけ割り当てることができます。
正解: **(正解を表示します)**
FortiSASE 7.6 管理ガイドおよび FCP - FortiSASE 24/25 管理者カリキュラムによると、セキュリティ ポスチャ タグ (ZTNA タグと呼ばれることが多い) は、ID ベースおよびポスチャ ベースのアクセス制御の基本的な構成要素です。
* 複数のタグの割り当て :1 つのエンドポイントに複数のタグを同時に割り当てることができます。たとえば、エンドポイントには「OS-Windows-11」、「AV-Running」、「Corporate-Domain-Joined」というタグが同時に付与される場合があります。
* 評価ロジック: ポリシー評価プロセス (SIA と SPA の両方) では、FortiSASE または FortiGate ハブがエンドポイントに割り当てられたすべてのタグを考慮します。セキュリティ ポリシーは、これらのタグをソース基準として使用するように構成できます。管理者が「AV 実行中」と「Corporate-Domain-Joined」の場合、システムは両方のタグを評価して、トラフィックを許可するかどうかを決定します。
* 動的な性質 :オプションCとは異なり、これらのタグは非常に動的です。FortiClientからSASEクラウドに送信されるテレメトリデータに基づいて、リアルタイムで自動的に適用または削除されます。ユーザーがウイルス対策ソフトを無効にすると、「AV-Running」タグは即座に削除され、エンドポイントのアクセス権は次回のポリシー評価で取り消されます。
* スケーラビリティ :システムは多くのタグをサポートしていますが、ドキュメントでは最適なパフォーマンスのためにカスタムタグのベースラインを推奨しています。ただし、包括的なセキュリティ体制を反映するには複数のタグが標準であると明記されています。
他の選択肢が間違っている理由：
* オプション A : これは誤りです。システムはタグを 1 つだけ選択するのではなく、タグのコレクションをポリシーの要件 (たとえば、いずれかに一致するか、すべてに一致するか) に照らして評価します。
* オプション C : これは誤りです。タグは動的であり、エンドポイントの状態 (脆弱性の数やソフトウェアの存在など) が変化するとすぐに変更されます。
* オプション D : これは誤りです。ZTNA のアーキテクチャ上の利点は、単一のユーザーに対して複数のセキュリティ「チェック」タグ）を階層化できることです。

質問: **22**
展示資料を参照してください。



SD-WANルールのステータスと設定が表示されています。この図に基づいて、測定されたレイテンシのどの変化によって、HUB1-VPN3が優先メンバーとして選択されるようになるでしょうか？

A. HUB1-VPN3の遅延が80msの場合

B. HUB1-VPN3のレイテンシがHUB1-VPN1およびHUB1-VPN2よりも低い場合

C. HUB1-VPN1の遅延が200msの場合

D. HUB1-VPN3の遅延が90msの場合

正解: **A** (コメントを発表する)

SD-WAN 7.6 コア管理者向け学習ガイドおよび FortiOS 7.6 管理ガイドによると、最良品質（優先度）ルールにおける優先メンバーの選択は、測定された品質メトリック（この場合は遅延）とリンクコストしきい値によって決定されます。

* ルールロジック（最高品質）：図は、SD-WANルールは設定モード優先度で構成されており、これは最高品質戦略に対応しています。この戦略では、リンクコスト係数（遅延に設定）に基づいてメンバーのランク付けが行われます。

* リンクコストしきい値: 図には、デフォルト値である 10% の値である link-cost-threshold(10) が示されています。

このしきい値は、「リンクフラッピング」を防ぐために設定されています。現在優先されているメンバーを置き換えるには、新しいメンバーはレイテンシが優れているだけでなく、10%以上優れている必要があります。

* 計算方法：

* 現在優先されているメンバーはHUB1-VPN1で、実際の遅延は96.349msです。

* 優先順位の低いメンバーが引き継ぐために達成しなければならない「目標」レイテンシを計算するには、次の式を使用します。$Target = \frac{Current_Latency}{(1 + \frac{Threshold}{100})}$。

* $\frac{96.349}{1.1} = \mathbf{87.59\text{ ms}}$。

* オプションの評価：

* オプション A (80 ms): 80 ms は必要な目標値 87.59 ms よりも低いため、HUB1-VPN3 は HUB1-VPN1 の 10% の優位性を克服し、新しい優先メンバーとなります。
* オプション D (90 ms): 90 ms は 96.349 ms より低いですが、87.59 ms より低くはありません。そのため、10% のしきい値によりメンバーの切り替えが防止され、HUB1-VPN1 が優先されます。
* オプションB :10%のしきい値があるため、〖レイテンシが低い」だけでは不十分なので、これは誤りです。
* オプション C: HUB1-VPN1 が 200 ms に移動した場合、HUB1-VPN2 (141.278 ms) が HUB1-VPN3 (190.984 ms) よりも優先されるメンバーになる可能性が高いです。

質問: **23**
FortiGateデバイスは、ルート検索プロセス中に、左の列に示されている以下の要素をどのような順序で考慮しますか？
左側の列の要素を選択し、ドラッグして右側の列の空いている位置に移動します。正しい要素を4つ順番に配置し、最初の要素を列の一番上の最初の位置に配置します。要素を配置した後、次の質問に進む前に回答を変更したい場合は、要素を再度移動できます。作業領域に4つの要素を配置する必要があります。
画面の区切り線を選択してドラッグすると、ソース領域と作業領域の表示範囲を変更できます。



正解:





質問: **24**
FortiSASEにおけるFortiViewの主な機能は何ですか？
A. 生のログデータをグラフ形式でのみ表示し、ソート条件や集計ビューは表示しません。
B. セキュリティイベントに関するリアルタイムアラートを生成し、メタデータなしで単一のテキストベースのコンソールに表示します。
C. 集計せずに個々のログをGUIに表示し、管理者がイベントを時間のみでソートできるようにします。
D. グラフィカルまたはテキストベースのログビューを使用して、時間の経過に伴うセキュリティイベントを分析するための統合コンソールを提供します。
正解: **(**正解を表示します**)**
FortiSASE上のFortiViewは、セキュリティイベントを時系列で統合した視覚的およびテキストベースのビューを提供し、管理者が集約されたダッシュボードを通じてログデータを効率的に分析および解釈できるようにします。

質問: **25**
ドラッグアンドドロップ
FortiGateデバイスは、ルート検索プロセス中に、左の列に示されている以下の要素をどのような順序で考慮しますか？



正解:



jpnshiken.com

Explanation:
1. 政策ルート
2. SD-WANのルール
3. 接続ルート
4. インターネットサービスデータベース（ISDB）ルート
FortiGateは、階層的な順序でルートを評価します。まずポリシー ルートをチェックし、次にSD-WANルールが有効になっている場合はそのルールをチェックします。その後、接続済みルートを評価し、続いてインターネット サービス用のISDBルートを評価し、最後に、より具体的な一致が見つからない場合はデフォルト ルートを評価します。

質問**: 26**
図を参照してください。FortiGateは、送信元IPアドレスが10.0.1.130、宛先IPアドレスが128.66.0.125のトラフィックをどのように処理しますか？

FortiGate router policy and diagnose output

```
branch1_fgt # show router policy
config router policy
     edit 1
          set src "10.0.1.128/255.255.255.128"
          set dst "128.66.0.0/255.255.255.0"
          set action deny
     next
end

branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
use-shortcut
     Tie break: cfg
     Shortcut priority: 2
          Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst
(1->65535), Mode(priority),
          link-cost-factor(latency), link-cost-threshold(10),
health-check(Corp_HC)
          Members(2):
               1: Seq_num(2 port2 underlay), alive, latency:
0.769, selected
               2: Seq_num(1 port1 underlay), alive, latency:
71.022, selected
          Application Control(3): Microsoft.Portal(41469,0)
Salesforce(16920,0) Collaboration (0,28)
          Src address(1):
               10.0.1.0-10.0.1.255

Service(4): Address Mode(IPV4) flags=0x24200 use-shortcut-sla
use-shortcut
     Tie break: cfg
     Shortcut priority: 2
          Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst
(1->65535), Mode(sla hash-mode=round-robin),
          Members(2):
               1: Seq_num(1 port1 underlay), alive sla(0x1),
gid(2), num of pass(1), selected
               2: Seq_num(2 port2 underlay), alive sla(0x1),
gid(2), num of pass(1), selected
          Src address(1):
               10.0.1.0-10.0.1.255
```

Jonshiken.com

```
        Dat address(1):
             128.66.0.0-128.66.255.255
```

A. FortiGateはポート2を通してトラフィックの流れを制御します。
B. FortiGateはFIBに従ってトラフィックフローをルーティングします。
C. FortiGateはポート1とポート2を通るトラフィックフローの負荷分散を行います。
D. FortiGate がトラフィックの流れを遮断します。
正解: **(**正解を表示します**)**
FortiGateでは、アクションが拒否のポリシー ルート (PBR) はトラフィックを即座に破棄しません。代わりに、そのポリシー ルートによるトラフィックのルーティングを阻止し、パケットは通常のルーティング 検索 (FIB) に返されます。
ソース10.0.1.130は10.0.1.128/25と一致します
宛先128.66.0.125は128.66.0.0/24と一致します
ルーターポリシーでは、アクション拒否→このポリシールートを使用しないように指示されています。
結果 :FortiGateはFIB（通常のルーティングテーブル）にフォールバックします。

質問: **27**
SD-WANルールの状態と構成を示す図を参照してください。

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority:2
      Gen(43), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
       link-cost-factor(packet loss), link-cost-threshold(0), heath-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, packet loss: 2.000%, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, packet loss: 4.000%, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), alive, packet loss: 12.000%, selected
     Src address(1):
          10.0.1.0-10.0.1.255

     Dst address(1):
          10.0.0.0-10.255.255.255

branch1_fgt (service) # show
config service
     edit 3
          set name "Corp"
          set mode priority
          set dst "Corp-net"
          set src "LAN-net"
          set health-check "HUB1_HC"
          set link-cost-factor packet-loss
          set link-cost-threshold 0
          set priority-members 6 4 5
     next
```

展示図に基づくと、測定されたパケット損失のどの変化によってHUB1-VPN3が新たな優先メンバーになるでしょうか？（回答を1つ選択してください）

A. 3つのメンバーすべてでパケット損失が同じ場合

B. HUB1-VPN1でパケット損失率が4%の場合

C. HUB1-VPN1でパケット損失率が12%の場合

D. HUB1-VPN3でパケット損失率が4%の場合

正解: **(**正解を表示します**)**

SD-WAN 7.6 Core Administrator 学習ガイドおよび FortiOS 7.6 管理ガイドによると、

最高品質（優先度）戦略選択プロセスは、測定されたリンク品質指標と構成されたメンバーの優先度順序という2つの主要な要素に依存します。

提供された資料（image_b40dfc.png）に基づいて、以下のことが分かります。

* 戦略と指標: このルールは、リンクコスト係数(パケット損失)を使用して、モード(優先度)(最高品質)で実行されます。

* 厳密な比較 :リンクコストしきい値は0に設定されます。これは、現在の優先リンクに「優位性」が与えられないことを意味し、FortiGateは厳密な比較を実行し、客観的に最も優れたメトリックを持つリンクを選択します。

* タイブレーカーロジック：複数のリンクでパケット損失が同じ場合、FortiGate はルール (set priority-members 6 4 5) で定義されたメンバー優先順位をタイブレーカーとして使用します。

FORTINET
jpnshiken.com

* メンバー6（HUB1-VPN3）が最優先です。
* メンバー4（HUB1-VPN1）は2番目の優先順位です。
* メンバー5（HUB1-VPN2）は最も優先順位が低い。
* 現在の状態：HUB1-VPN1は、パケット損失率（2.000%）がHUB1-VPN2（4.000%）およびHUB1-VPN3（12.000%）よりも低いため、現在選択されています。HUB1-VPN3は設定優先度が高いものの、パケット損失率が著しく高いため選択されません。
オプションの評価：
* オプション A (検証済み): 3 つのメンバーすべてでパケット損失率が同じ場合 (たとえば、すべて 2%)、品質指標は同等です。SD-WAN エンジンは、優先メンバーリストを参照します。HUB1-VPN3 (Seq 6) はそのリストの最初のメンバーであるため、すぐに新しい優先メンバーになります。
* オプションB：HUB1-VPN1が4%に達した場合、HUB1-VPN2（4%）と一致させます。HUB1-VPN3は12%のままです。
システムはVPN1とVPN2のどちらかを選択します。VPN1（シーケンス4）はVPN2（シーケンス5）よりも優先順位が高いため、HUB1-VPN1が優先されます。
* オプションC：HUB1-VPN1が12%に達した場合、HUB1-VPN3と同等になります。しかし、HUB1-VPN2は4.000%と依然として優れています。したがって、HUB1-VPN3ではなく、HUB1-VPN2が新しい優先メンバーになります。
* オプション D：HUB1-VPN3 が 4% に低下した場合、HUB1-VPN2 と一致します。ただし、HUB1-VPN1 は依然として 2.000% で最適なリンクであるため、選択されたままになります。

質問: **28**
展示資料を参照してください。

FortiGate router policy and diagnose output

```
branch1_fgt # show router policy
config router policy
    edit 1
        set src "10.0.1.128/255.255.255.128"
        set dst "128.66.0.0/255.255.255.0"
        set action deny
    next
end

branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
 Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), health-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.769, selected
    2: Seq_num(1 port1 underlay), alive, latency: 71.022, selected
  Application Control(3): Microsoft.Portal(41469,0) Salesforce(16920,0) Collaboration(0,28)
  Src address(1):
        10.0.1.0-10.0.1.255

Service(4): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla  hash-mode=round-robin)
  Members(2):
    1: Seq_num(1 port1 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(2 port2 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        128.66.0.0-128.66.255.255
```

FORTINET
jpns-hiken.com

FortiGateは、送信元IPアドレスが10.0.1 130、宛先IPアドレスが128 66.0 125のトラフィックをどのように処理しますか？
A. FortiGateはポート2を介してトラフィックの流れを制御します
B. FortiGateがトラフィックフローをドロップします

C. FortiGateはFIBに従ってトラフィックフローをルーティングします。
D. FortiGateはポート1とポート2を介したトラフィックフローを負荷分散します
正解: (正解を表示します)
正解はCです。FortiGateはFIBに従ってトラフィックフローをルーティングします。図は、送信元10.0.1.128/255.255.255.128、宛先128.66.0.0/255.255.255.0で構成された通常のポリシー ルートを示しています。
テストソース 10.0.1.130 は 10.0.1.128/25 サブネットに属し、宛先 128.66.0.125 は
128.66.0.0/24。したがって、トラフィックはこのポリシールートに一致します。
重要な点として、このルートには 「拒否」アクションが設定されています。ルーターポリシーの場合、これはファイアウォールの 「拒否」のようにFortiGateがパケットを破棄することを意味するものではありません。これは 「ポリシールーティングの停止」を表します。Fortinetの説明によると、パケットがこのアクションに一致すると、FortiGateはポリシールーティング処理を停止し、転送情報ベース (FIB) を使用してパケットをルーティングします。
通常のポリシー ルートは、SD-WAN ルールよりも優先されます。したがって、図に示す SD-WAN サービス 4 は、送信元 10.0.1.0～10.0.1.255、宛先 128.66.0.0～128.66.255.255 に一致しますが、ポート 1 とポート 2 のラウンド ロビン選択はこのフローを制御しません。一致する通常のポリシー ルートが、ポリシー ルーティングを先に終了します。
学習ガイド参照 :SD-WAN構成と監視 > ポリシールート > ルート検索とFIB処理、423～424ページ。

質問: **29**
ユーザーのノートパソコンにFortiClientをインストールするために使用される配信方法はどれですか？ (2つ選択してください。)
A. FortiSASEポータルからインストーラーを直接ダウンロードしてください。
B. API を介してユーザーのノートパソコンに自動インストールを設定します。
C. FortiClientインストーラーへのリンクを含む招待メールを、選択したユーザーに送信します。
D. サードパーティのアプリケーションストアからゼロタッチインストールを使用します。
正解: (正解を表示します)

質問: **30**
トラフィックが暗黙のSD-WANルールに一致した場合に何が起こるかを正しく説明しているのは、次のうちどの2つの記述ですか？
(2つ選択してください)
A. トラフィックは、v4-ecmp-mode 設定で設定されたアルゴリズムを使用して負荷分散されます。
B. トラフィックがポリシー経路テーブルのエントリのいずれにも一致しません。
C. FortiGate はセッションに may_dirty と vwl_default のフラグを付けます。
D. トラフィックは、重量に関係なく、利用可能なすべての静的ルートに分散されます。
E. セッション情報出力にSD-WANサービスIDが表示されません。
正解: (正解を表示します)
SD-WAN 7.6 Core Administrators学習ガイドおよびFortiOS 7.6管理ガイドによると、
「暗黙のルール」は、SD-WANルールリストの一番下にあるデフォルトルール (ID 0) です。このルールは、トラフィックが手動で設定されたSD-WANルールのいずれにも一致しない場合にのみ評価されます。
* ポリシールーティングテーブルのコンテキスト (オプションB) SD-WANルールは、技術的にはポリシーベースルーティングの特殊な形式です。パケットが暗黙のルールに一致するには、まずルーティング階層を通過する必要があります。トラフィックが暗黙のルールに一致する場合、それは、トラフィックを以前に遮断するはずだった、より優先度の高いユーザー定義のSD-WANルールや、手動ポリシールーティングテーブルの特定のエントリに一致しなかったことを示します。
* セッション情報 (オプション E): CLI を使用してアクティブなセッションを検査する場合 (例: diagnose sys session list)、出力には SD-WAN サービス ID の

フィールドが含まれます。トラフィックがユーザー定義ルールによってルーティングされている場合、そのルールの ID (例: service_id=1) が表示されます。ただし、トラフィックが暗黙のルールにフォールスルーする場合、セッション情報には SD-WAN サービス ID は表示されません (多くの場合 0 と表示されるか、省略されます)。これは、暗黙のルールがユーザー定義ルールと同じように 「サービス」として機能しないためです。
* ルーティング動作: 暗黙のルールは、標準のルーティングテーブル (RIB/FIB) ロジックに従います。静的ルートの優先度と距離を使用してパスを決定します。複数のパスが同じ距離と優先度を持つ場合、v4-ecmp-mode で設定されたアルゴリズムを使用しますが、これはルーティングエンジンの機能であり、SD-WAN エンジン自体の機能ではありません。
他の選択肢が間違っている理由：
* オプション A: v4-ecmp-mode (ソース IP ベース) は ECMP ルーティングに使用されますが、これは FIB 内の等コストパスの一般的な FortiOS ルーティング動作の一部であり、暗黙のルールは単に
決定権をそのルーティングテーブルに 「委ねる」。
* オプション C: トラフィックが暗黙のルールに一致すると、セッションは実際には vwl_id=0 でフラグ付けされ、ルート変更が発生するとダーティになる可能性がありますが、vwl_default はカリキュラムのこの特定のコンテキストで使用される標準のフラグ名ではありません。
* オプション D: これは誤りです。暗黙のルールは、ルーティング テーブル内の静的ルートで定義されている重み、距離、優先度を尊重します。これらの値に関係なくトラフィックを分散するわけではありません。

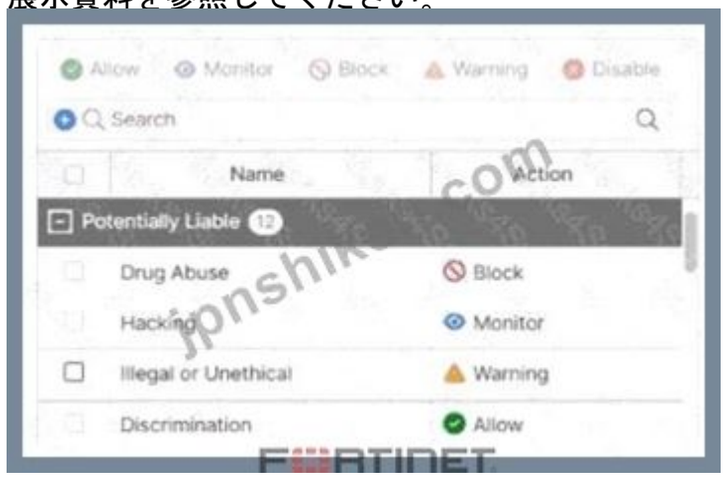
質問: **31**
FortiSASEにおけるオンネット／オフネットルール設定の目的は何ですか？
A. 外部ネットワークアクセスに対するユーザー認証を有効または無効にします。
B. オンプレミスとクラウドベースのリソースに対して、異なるトラフィックルーティングルールを定義する。
C. エンドポイントが信頼できるネットワークから接続しているか、信頼できない場所から接続しているかを判断します。
D. ユーザーの地理的位置に基づいて、異なるアクセス ポリシーを設定します。
正解: **(正解を表示します)**
FortiSASEのオン/オフネットルール設定では、エンドポイントをオンネット（支店などの信頼できる企業ネットワーク内）またはオフネット（自宅や公共Wi-Fiなどの遠隔地または信頼できない場所）に分類します。
管理者は、IPサブネット、ゲートウェイMACアドレス、またはその他の基準を使用してオンネットルールを定義し、FortiSASEの自動接続からオンネットエンドポイントを除外したり、異なるプロファイルを適用したりするなどの動作をトリガーします。

有効的な**NSE5_SSE_AD-7.6**問題集はJPNTest.com提供され、**NSE5_SSE_AD-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE5_SSE_AD-7.6**試験問題集を提供します。JPNTest.com NSE5_SSE_AD-7.6試験問題集はもう更新されました。ここで**NSE5_SSE_AD-7.6**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/NSE5_SSE_AD-7.6-mondaishu **50**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
FortiSASEでステアリングバイパスの宛先を設定することに関する記述のうち、正しいものはどれですか？ 2つ選択）
2つ選択してください。）
A. インフラストラクチャ、FQDN、ローカルアプリケーション、サブネットの4つの宛先タイプから選択できます。
B. 条件を適用すると、分割トンネル宛先をオンネット、オフネット、または両方のタイプのエンドポイントに適用できます。
C. サブネットは、適用条件をサポートする唯一の宛先タイプです。

D. 適用条件は、オンネットまたはオフネットのいずれか一方のみに設定でき、両方には設定できません。
正解: (正解を表示します)
ステアリングバイパスの宛先は、インフラストラクチャ、FQDN、ローカルアプリケーション、サブネットの4種類の宛先タイプをサポートしています。
適用条件は、バイパスがオンネット、オフネット、または両方のエンドポイント状態に適用されるかどうかを決定します。

質問: **33**
展示資料を参照してください。

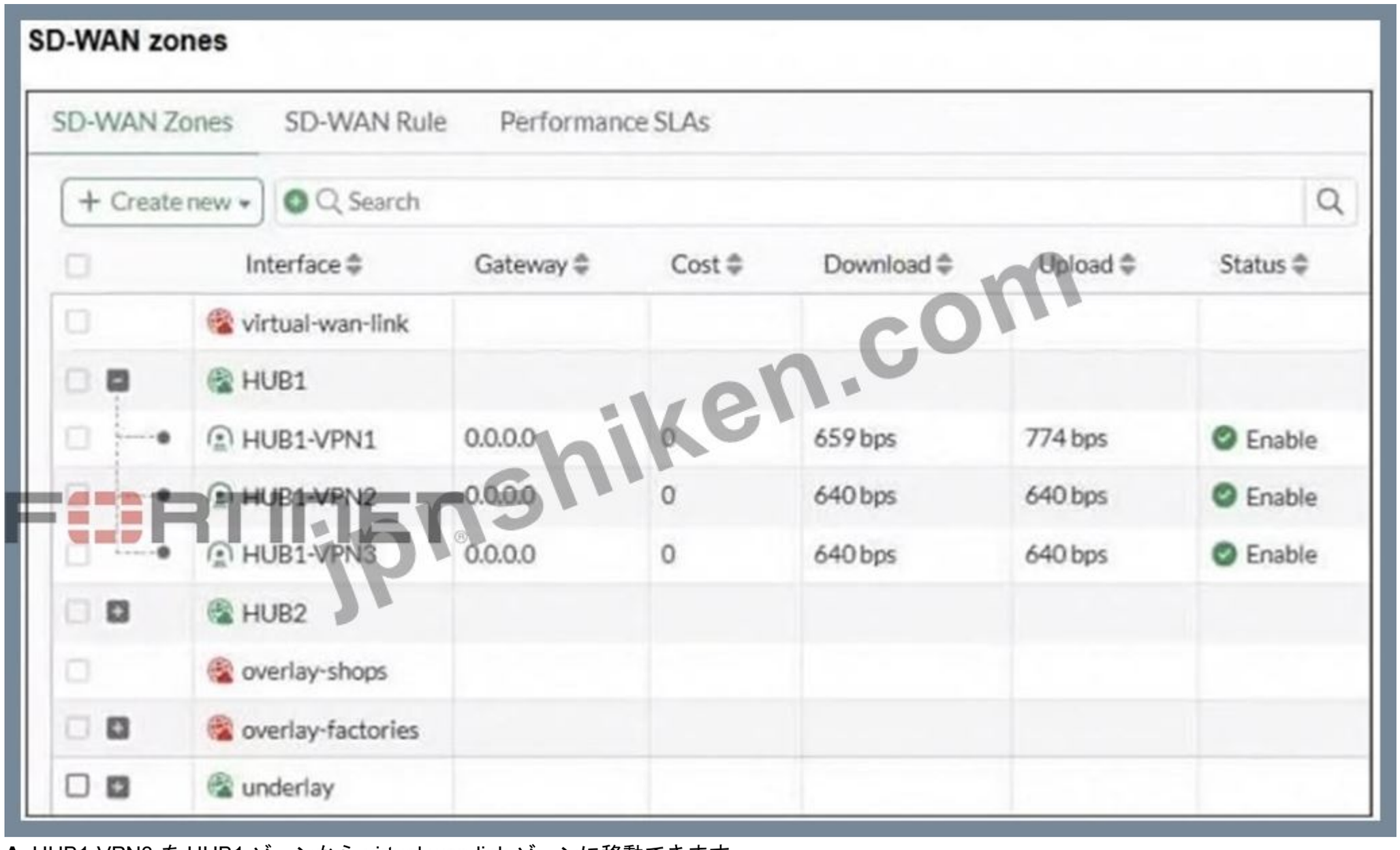


どのウェブフィルタカテゴリへのアクセスが拒否され、ユーザーに代替メッセージが表示されますか？
A. 薬物乱用
B. 差別
C. ハッキング
D. 違法または非倫理的
正解: (正解を表示します)
正解は A. 薬物乱用です。図では、FortiGuard Webフィルタカテゴリ 「薬物乱用」がブロックアクションで設定されています。FortiSASEは、要求されたWebサイトに割り当てられたFortiGuardカテゴリに従って、設定されたアクションを適用します。FortiSASE管理者学習ガイドでは、ブロックは、設定されたカテゴリに属するURLへのアクセスを拒否し、代替メッセージを表示するアクションとして明示的に定義されています。
表示されている他のカテゴリは、それぞれ異なる動作をします。ハッキングは 「監視」に設定されており、トラフィックの処理は 「許可」と同様ですが、一致するトラフィックが検出されるたびにログエントリが生成されます。そのため、ユーザーのアクセスは拒否されません。違法または非倫理的なトラフィックは 「警告」に設定されており、警告ページが表示されますが、ユーザーが選択すれば続行できます。差別は 「許可」に設定されているため、トラフィックは残りの検査エンジンを通過し、ブロックされません。
したがって、この展示では、要求された動作 「アクセスを拒否し、代替メッセージを表示する」がブロックアクションに直接マッピングされており、薬物乱用は、そのように設定されている唯一のカテゴリです。
学習ガイド参照 :セキュリティとエンドポイントプロファイル > インラインCASBを使用したWebフィルタ > FortiGuardカテゴリフィルタ、118ページ。

質問: **34**
FortiSASEにおけるセキュリティ態勢タグに関する記述として正しいのはどれですか？
A. エンドポイントには複数のタグを割り当てることができますが、評価に使用されるのは1つだけです。
B. エンドポイントに複数のタグを割り当てて評価に使用できます。
C. タグは静的であり、エンドポイントの状態によって変更されません。
D. エンドポイントにはタグを1つだけ割り当てることができます。

正解: (正解を表示します)
FortiSASEのセキュリティ態勢タグは、OSバージョン、ウイルス対策ソフトの状態、FortiClientの接続状況などのルールに基づいて、エンドポイントのコンプライアンスを動的に評価します。エンドポイントは複数のタグ（Windows 11、アクティブなウイルス対策ソフト、SASE接続など）を同時に受信し、ファイアウォールはこれらのタグをZTNAアクセス制御ポリシーに基づいて評価します。

質問: **35**
図を参照してください。FortiGateのGUIにおけるSD-WANゾーンの設定例を示します。
このデバイスのゾーンとメンバーの設定について、どのような結論が得られますか？



A. HUB1-VPN3 を HUB1 ゾーンから virtual-wan-link ゾーンに移動できます。
B. オーバーレイ工場ゾーンにはメンバーがいません。
C. 仮想WANリンクゾーンを削除できます。
D. オーバーレイファクトリーゾーンを削除できます。
正解: (正解を表示します)
SD-WANゾーンビューでは、overlay-factoriesゾーンの下に展開可能な矢印やメンバーインターフェイスが表示されないため、このゾーンにはメンバーが含まれていないことがわかります。

質問: **36**
FortiSASE GeofencingにおけるVPN接続管理のための優先接続／フェイルオーバー接続機能の目的は何ですか？
A. リモートユーザーは場所に関係なく、最寄りのセキュリティPOPにのみ接続するように強制されます。
B. 管理者は、特定の国のユーザーに対してオンプレミスの FortiGate 接続を優先するルールを定義でき、FortiGate デバイスが利用できない場合はセキュリティ POP にフェイルオーバーします。
C. ユーザーの地理的位置に基づいてVPNアクセスを制限し、フェイルオーバーオプションを許可しません。
D. オンプレミスデバイスを優先することなく、利用可能なすべてのセキュリティPOP間でVPNトラフィックを自動的にバランス調整します。
正解: **(正解を表示します)**
FortiSASEのジオフェンシングにおける優先順位/フェイルオーバー機能を使用すると、管理者は特定の国のユーザーに対してオンプレミスのFortiGateを優先し、オンプレミスのデバイスにアクセスできない場合にのみFortiSASEセキュリティPOPにフェイルオーバーすることができます。

質問: **37**
展示資料を参照してください。

Diagnose output

```
fgt_1 # diagnose  sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
 link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.906, selected
    2: Seq_num(1 port1 underlay), alive, latency: 1.079, selected
  Application Control(2): Microsoft.Portal(41469,0) Business(0,29)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla
hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HQ_T1 overlay), alive, sla(0x3), gid(0), cfg_order(0),
local cost(0), selected
    2: Seq_num(5 HQ_T2 overlay), alive, sla(0x3), gid(0), cfg_order(1),
local cost(0), selected
    3: Seq_num(6 HQ_T3 overlay), alive, sla(0x3), gid(0), cfg_order(2),
local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

この展示は、FortiGateデバイス上で収集されたコマンド「diagnose sys sdwan service」の出力結果を示しています。

管理者は、FortiGateがサブネット10.0.1.0/255.255.255.192上のローカルユーザーからのトラフィックを、ソーシャルメディアアプリケーションFacebook宛てにどのインターフェース経由でルーティングするかを知りたいと考えています。

展示物に基づいて、正しい記述は次のうちどれですか？（2つ選択してください。）

A. FortiGateは、サービスルール2に従ってソーシャルメディアアプリケーションのトラフィックをルーティングし、ポート2を介してトラフィックをルーティングします。

B. Facebook アプリケーションにはサービスが定義されていないため、FortiGate はサービス ルール 3 を適用し、トラフィックを本社に転送します。

C. FortiGateがフローのアプリケーションを認識できない場合、HQ_T1、HQ_T2、HQ_T3トンネルを介してトラフィックを負荷分散します。

D. FortiGate がフローのアプリケーションを認識できない場合、ルール 3 の優先メンバーである HQ_T1 を介してトラフィックをルーティングします。

正解: **A,C** (コメントを発表する)

「フローが定義済みのアプリケーションカテゴリ（ソーシャルメディアなど）に属すると識別された場合、FortiGateはそれを対応するサービスルール（ルール2）に照

FORTINET
jpnshiken.com

合し、ポート2などの指定されたインターフェースを通してルーティングします。」
ただし、セッション設定中にアプリケーションが認識されない場合、システムはデフォルトで、未分類トラフィックのポリシーに従って利用可能なトンネルを使用してトラフィックの負荷分散を行い、アプリケーションの分類を待っている間も継続的な接続を確保します。これにより、パフォーマンスと回復力の両方が保証されます。

質問: **38**
FortiSASEで有効なレポートタイプはどれですか？ （3つ選択してください。）
A. シャドウITレポート
B. エンドポイントコンプライアンス逸脱レポート
C. サイバー脅威評価
D. 脆弱性評価レポート
E. ウェブ利用状況サマリーレポート
正解: **A,D,E (**コメントを発表する**)**
シャドウITレポート :このレポートは、組み込みのCASB（クラウドアクセスセキュリティブローカー）機能を活用し、従業員が使用している「承認されていない」または「リスクの高い」SaaSアプリケーションを特定します。IT部門によって明示的に承認されていないクラウドアプリケーションを一覧化することで、組織が潜在的なセキュリティリスクを発見するのに役立ちます。
脆弱性評価レポート :FortiSASEはFortiClientおよび組み込みEMSと統合されているため、管理対象エンドポイントからの脆弱性スキャンデータを集約できます。このレポートには、ユーザーデバイス（OSレベルおよびアプリケーションレベル）で検出されたソフトウェアの脆弱性が一覧表示され、ゼロトラストネットワークアクセス（ZTNA）の実施に不可欠な「セキュリティ評価」またはセキュリティ態勢評価が提供されます。
ウェブ利用状況概要レポート :このレポートは、SASE環境全体におけるウェブアクティビティの概要を分かりやすく示します。ウェブサイトのカテゴリー（ソーシャルメディア、ストリーミング、悪意のあるサイトなど）、帯域幅上位ユーザー、ブロックされたリクエストなど、トラフィックを分類することで、ITチームがリモートワーカーによるインターネットリソースの消費状況を把握するのに役立ちます。

質問: **39**
エンドポイントアップグレードルールを使用してFortiClientのアップグレードをスケジュールすることに関して、正しい記述はどれですか？
A. スケジュールされている場合、エンドポイントがオンラインであれば、インストールは常にすぐに開始されます。
B. エンドポイントのアップグレードルールは、ユーザーグループに割り当てることができます。
C. スケジュールされたアップグレードでは、インストール後にmacOSエンドポイントが自動的に再起動されます。
D. エンドポイントの現地時間で予定時刻が既に過ぎている場合、インストールは翌日のその時刻に開始されます。
正解: **D (**コメントを発表する**)**
FortiClientのアップグレードは、エンドポイントの現地時間に基づいて実行されます。そのタイムゾーンで予定時刻が既に過ぎている場合は、アップグレードは翌日の同じ時刻まで延期されます。

質問: **40**
展示資料を参照してください。



SD-WANルールのステータスと設定が表示されています。この図に基づいて、測定されたレイテンシのどの変化によって、HUB1-VPN3が優先メンバーとして選択されるようになるでしょうか？

A. HUB1-VPN3の遅延が80msの場合
B. HUB1-VPN3のレイテンシがHUB1-VPN1およびHUB1-VPN2よりも低い場合
C. HUB1-VPN1の遅延が200msの場合
D. HUB1-VPN3の遅延が90msの場合
正解: **(**正解を表示します**)**
SD-WAN 7.6 Core Administrator 学習ガイドおよび FortiOS 7.6 管理ガイドによると、最良品質 (優先度) ルールにおける優先メンバーの選択は、測定された品質メトリック (この場合は遅延) とリンクコストしきい値によって決定されます。
ルールロジック（最高品質）：図は、SD-WANルールは設定モード優先度で構成されており、これは最高品質戦略に対応しています。この戦略では、リンクコスト係数（レイテンシに設定）に基づいてメンバーのランク付けが行われます。
リンクコストしきい値：図には、デフォルト値である10%のlink-cost-threshold(10)が示されています。このしきい値は、「リンクフラッピング」を防ぐために設定されています。現在の優先メンバーを置き換えるには、新しいメンバーはレイテンシが優れているだけでなく、10%以上優れている必要があります。
計算方法：
現在最も推奨されているメンバーはHUB1-VPN1で、実遅延は96.349msです。
優先度の低いメンバーが引き継ぎを行うために達成しなければならない「目標」レイテンシを計算するには、次の式を使用します。
$Target = \frac{Current_Latency}{(1 + \frac{Threshold}{100})}$。
$\frac{96.349}{1.1} = \mathbf{87.59\text{ ms}}$.
選択肢の評価：
オプションA（80ms）80msは要求される目標値87.59msよりも低いため、HUB1-VPN3はHUB1-VPN1の10%の優位性を克服し、新たな優先メンバーとなります。
オプションD（90ms）90msは96.349msより低いものの、87.59msより低くはありません。そのため、10%のしきい値によりメンバーの切り替えは行われず、HUB1-VPN1が優先されます。

選択肢B :10%のしきい値があるため、「レイテンシが低い」だけでは不十分なので、誤りです。
オプションC :HUB1-VPN1が200msに移動した場合、HUB1-VPN2（141.278ms）がHUB1-VPN3（190.984ms）よりも先に新しい優先メンバーになる可能性が高い。

質問: **41**
展示資料を参照してください。



SD-WANルールのステータスと設定が表示されています。この図に基づいて、測定されたレイテンシのどの変化によって、HUB1-VPN3が優先メンバーとして選択されるようになるでしょうか？
A. HUB1-VPN3の遅延が80msの場合
B. HUB1-VPN3のレイテンシがHUB1-VPN1およびHUB1-VPN2よりも低い場合
C. HUB1-VPN1の遅延が200msの場合
D. HUB1-VPN3の遅延が90msの場合
正解: **A** (コメントを発表する)
SD-WAN 7.6 Core Administrator 学習ガイドおよび FortiOS 7.6 管理ガイドによると、
ベストクオリティ（優先度）ルールにおける優先メンバーの選択は、測定された品質メトリック（この場合は遅延）とリンクコストしきい値によって決定されます。
* ルールロジック (最高品質): 図では、SD-WAN ルールは設定モード優先度で構成されており、これは最高品質戦略に対応しています。この戦略では、リンクコスト係数に基づいてメンバーのランク付けが行われ、リンクコスト係数は遅延に設定されています。
* リンクコストしきい値：図には、デフォルト値である 10% の値である link-cost-threshold(10) が示されています。
このしきい値は、「リンクフラッピング」を防ぐために設定されています。現在の優先メンバーを置き換えるには、新しいメンバーはレイテンシが優れているだけでなく、10%以上優れている必要があります。
* 計算方法：
* 現在の優先メンバーはHUB1-VPN1で、実際の遅延は96.349msです。
* 優先順位の低いメンバーが引き継ぐために達成しなければならない「目標」レイテンシを計算するには、次の式を使用します。$Target = \frac{Current_Latency}{(1 + \frac{Threshold}{100})}$。

* $\frac{96.349}{1.1} = \mathbf{87.59\text{ ms}}$。
* オプションの評価：
* オプション A (80 ms) : 80 ms は必要な目標値 87.59 ms よりも低いため、HUB1-VPN3 は HUB1-VPN1 の 10% の優位性を克服し、新しい優先メンバーとなります。
* オプション D (90 ms) : 90 ms は 96.349 ms より小さいですが、87.59 ms より小さくはありません。
したがって、10%のしきい値によってメンバーの切り替えが防止され、HUB1-VPN1が引き続き優先される。
* オプション B: 10% のしきい値があるため、「レイテンシが低い」だけでは不十分なので、不正解です。
* オプション C : HUB1-VPN1 が 200 ms に移動した場合、HUB1-VPN2 (141.278 ms) が HUB1-VPN3 (190.984 ms) よりも優先される可能性が高いです。

質問: **42**
FortiSASEのリモートユーザーに対する安全な本人確認とアクセス制御をサポートする認証ソースはどれですか？（3つ選択してください。）
A. セキュリティアサーションマークアップ言語（SAML）
B. OpenID Connect（OIDC）
C. 軽量ディレクトリアクセスプロトコル（LDAP）
D. ターミナルアクセスコントローラアクセス制御システムプラス（TACACS+）
E. リモート認証ダイヤルインユーザーサービス (RADIUS)
正解: **A,C,E (**コメントを発表する**)**
FortiSASEは、リモートユーザーの本人確認に適用可能な認証メカニズムとして、SAML、LDAP、およびRADIUSをサポートしています。FortiSASE管理者学習ガイドでは、認証サーバー構成の目的として、LDAPおよびRADIUSによるリモート認証とSAMLシングルサインオン（SSO）について明確に説明しています。さらに、FortiSASEは、ローカルデータベース、RADIUS、LDAP、およびSAMLによるSSO認証をサポートしていると述べています。
SAML（A）は、サービスプロバイダとして機能するFortiSASEが、ユーザー認証に外部のIDプロバイダを利用できるようにするため、フェデレーションSSOを提供します。SAML SSOは、FortiSASE SWGおよびVPNの展開において特にサポートされています。
LDAP（C）を使用すると、Microsoft Active Directoryなどのディレクトリサービスとの統合が可能になります。FortiSASEは、LDAPインフラストラクチャに対してディレクトリ情報を照会し、ユーザーを認証できます。また、保護された通信のためにLDAPSを有効にすることもできます。ガイドには重要な制限事項が記載されています。IPsec VPNを使用するSIAリモートユーザーはLDAP認証を利用できませんが、LDAPはFortiSASEの認証ソースとして引き続きサポートされています。
RADIUS（E）は、集中型のリモート認証を提供し、PAP、CHAP、MS-CHAP、およびMS-CHAPv2認証方式をサポートします。
このコースの目的において、OIDCおよびTACACS+はFortiSASE のリモートユーザー認証ソースとして指定されていません。

質問: **43**
ITチームは、今後のFortiClientのアップグレードにおいても、MDMツールを引き続き使用する必要があるかどうかを検討している。
FortiClientの今後のアップグレードに対応するために、どのような選択肢がありますか？
A. FortiSASEポータルでエンドポイントアップグレード機能を有効にします。
B. FortiClientは手動でアップグレードする必要があります。
C. 管理対象エンドポイントユーザーに対して、より新しいバージョンのFortiClientのオンボーディングを実行します。
D. より新しいFortiClientバージョンは、必要に応じて自動的にアップグレードされます。
正解: **(**正解を表示します**)**
FortiSASE 7.6機能管理ガイドおよびNSE 5 SASEカリキュラムの最新アップデートによると、FortiSASEはFortiClientエージェントのネイティブライフサイクル管理を導入し、これまでアップデートのたびにサードパーティ製のMDM（モバイルデバイス管理）またはGPO（グループポリシーオブジェクト）のみに依存していたITチームの運用負担を軽減しました。
FortiSASEポータルの「システム」>「エンドポイントアップグレード」にあるエンドポイントアップグレード機能を使用すると、管理者は次の操作を実行できます。

一元化されたバージョン管理：管理者は、現在展開されているバージョンと、FortiGuardから入手可能な「推奨」バージョンを確認できます。
スケジュールされたロールアウト：指定された時間にすべてのエンドポイントまたは特定のエンドポイントグループをアップグレードすることを選択できます。これにより、アップグレードが業務運営を中断しないようにすることができます。
ステータス監視：ポータルには、アップグレードの進行状況（ダウンロード中、インストール中、再起動待ち、成功など）をリアルタイムで表示するダッシュボードが用意されています。
手動 vs. マネージド：MDMは、最初のオンボーディング（FortiClientを初めてインストールしてSASEクラウドに接続する時）には依然として強く推奨されますが、それ以降のアップグレードはすべてFortiSASEポータルでネイティブに処理できます。
他の選択肢が間違っている理由：
オプションB：手動アップグレードは大規模な展開（このシナリオでは約400ユーザー）には非効率的であり、FortiSASEが提供する「機能豊富な」ソリューションとして意図されているものではありません。
オプションC：「オンボーディング」とは、初期設定のことです。バージョンが変更されるたびにオンボーディングをやり直すのは、無駄が多く非効率的です。
オプションD：システムはアップグレードを管理できますが、ポータルで管理者が設定を行わない限り、クライアント自身による「オンデマンドでの自動アップグレード」は行われません。管理者は、対象バージョンとスケジュールを定義する必要があります。

質問: **44**
FortiSASEがサポートする導入環境について、正しい記述はどれですか？
A. FortiSASEは、ユーザーの要件に基づいて、VPNモードとエージェントレスモードをサポートします。
B. FortiSASEは、展開状況に応じてエンドポイントモードとSWGモードの両方をサポートします。
C. FortiSASEはSWGモードでのみ動作し、すべてのトラフィックはFortiSASE POPを経由するように強制されます。
D. FortiSASEはZTNAのみのモードに依存しており、SWGとエンドポイント機能は置き換えられています。
正解: **B** (コメントを発表する)
FortiSASE 7.6 管理ガイドおよび FCP - FortiSASE 24/25 管理者カリキュラムによると、FortiSASE はさまざまなユーザーおよびデバイスの要件をサポートするためにハイブリッド展開アーキテクチャで設計されています。主に次の 2 つのモードで動作します。
* エンドポイントモード（エージェントベース）：このモードでは、ユーザーのラップトップまたはデバイスにFortiClientをインストールする必要があります。エージェントは、最寄りのFortiSASE Point of Presence（PoP）への「常時接続」のセキュアVPNトンネルを確立し、完全なセキュアインターネットアクセス（SIA）、セキュアプライベートアクセス（SPA）、およびエンドポイントの姿勢チェック（ZTNA）を提供します。
* セキュアWebゲートウェイ（SWG）モード（エージェントレス）：このモードは、エージェントのインストールが不可能なユーザーまたはデバイス（管理対象外デバイスやChromebookなど）に使用されます。明示的なWebプロキシ設定またはPAC（プロキシ自動構成）ファイルを使用して、Webトラフィック（HTTP/HTTPS）をSASE PoPにリダイレクトし、検査を行います。
他の選択肢が間違っている理由：
* オプション A : VPN をサポートしていますが、「VPN モード」は正式な展開タイプの名称ではなく、「エンドポイント モード」です。
* オプション C : FortiSASE は SWG に限定されず、FWaaS および ZTNA を含む完全な SSE (Security Service Edge) ソリューションです。
* オプション D : ZTNA はプラットフォーム内の機能であり、エンドポイントまたは SWG 機能の全体的な代替ではありません。

質問: **45**
SD-WANルールを設定する際に、SLA目標とSD-WANルールに関して考慮すべき3つの要素は何ですか？（3つ選択してください）
A. SD-WANルールを設定する際、異なるパフォーマンスSLAから複数のSLAターゲットを選択できます。
B. SLAターゲットは、最低コスト（SLA）戦略で構成されたSD-WANルールでのみ使用されます。
C. メンバーの指標は、ルールがSLAターゲットを使用している場合にのみ測定されます。

D. SD-WANルールはSLAターゲットを使用して、優先メンバーがSLA要件を満たしているかどうかを確認できます。
E. SD-WANルールを設定する際、同じパフォーマンスSLAに属する複数のSLAターゲットを選択できます。
正解: **(**正解を表示します**)**
SD-WAN 7.6 Core Administrator 学習ガイドおよび Fortinet ドキュメントライブラリによると、SD-WAN ルールと SLA ターゲット間の相互作用は、特定の選択および測定ロジックによって制御されます。
* 戦略による使用（オプション B）SLA ターゲットは、基本的に最低コスト（SLA）戦略によって使用され、トラフィック ステアリングの対象となるのに十分な健全性を持つリンクを決定します。
「最高品質」などの他の戦略では、指標を監視するために「測定SLA」を使用しますが、ハイブリッドモードで特別に設定されていない限り、「必須SLA目標」を使用してリンクを不適格とすることはありません。ほとんどのカリキュラムでは、「必須SLA目標」フィールドは、「最低コスト」および「帯域幅最大化」戦略に特に関連付けられています。
* SLA準拠チェック（オプションD）SD-WANルールは、SLAターゲットを「合格／不合格」判定のゲートキーパーとして利用します。エンジンは、優先メンバーが定義されたSLA要件（遅延、ジッター、パケット損失のしきい値）を満たしているかどうかを確認します。優先メンバーがSLAを満たさない場合、ルールはSLAを満たす優先順位リストの次のメンバーに移動します。
* 単一SLAバインディング（オプションE）SD-WANルールを設定する際、GUIとCLIでは複数のSLAターゲットを選択できますが、それらはすべて同じパフォーマンスSLAプロファイルに属している必要があります。単一のSD-WANルール内で、異なるヘルスチェックのターゲット（例：「Google_HC」のターゲット1と「Amazon_HC」のターゲット2）を混在させることはできません。
他の選択肢が間違っている理由：
* オプション A :これは誤りです。単一の SD-WAN ルールは、一度に 1 つの特定のパフォーマンス SLA プロファイルにのみ関連付けることができるため、異なる SLA からターゲットを選択することはできません。
* オプション C :これは誤りです。メンバーメトリック（レイテンシ、ジッター、パケット損失）は、SD-WAN ルールが現在その SLA ターゲットをステアリング決定に使用しているかどうかに関係なく、パフォーマンス SLA プローブによって測定されます。測定はヘルスチェックの機能であり、ルールマッチングプロセスの機能ではありません。

質問: **46**
FortiGateデバイスが稼働中です。WANリンクの使用効率を最適化し、冗長性を向上させるため、SD-WANを有効化して設定します。
この構成更新プロセスの一環として、必ず行うべきことは何ですか？（回答を1つ選択してください）
A. ファイアウォール ポリシーで SD-WAN メンバーとして使用されているインターフェイスへの参照を置き換えます。
B. ルーティング設定でSD-WANメンバーとして使用されているインターフェースへの参照を置き換えます。
C. SD-WANメンバーとして使用したいインターフェースを無効にします。
D. SD-WANライセンスを購入してインストールし、FortiGateデバイスを再起動します。
正解: **A (**コメントを発表する**)**
SD-WAN 7.6 コア管理者学習ガイドおよび FortiOS 7.6 管理ガイドによると、本番環境の FortiGate を SD-WAN を使用するように移行する場合、最も重要な手順は、トラフィックの許可方法とルーティング方法を再構成することです。
参照削除要件：インターフェース（wan1やwan2など）をSD-WANメンバーとして追加する前に、FortiGate構成のほとんどの部分で「参照されていない」状態にする必要があります。具体的には、インターフェースが現在アクティブなファイアウォールポリシーで使用されている場合、システムはそれをSD-WANバンドルに追加することを阻止します。
ファイアウォールポリシーの移行（オプションA）：運用環境は、ファイアウォールポリシー内の物理インターフェイスへの参照を、新しいSD-WAN仮想インターフェイス（またはSD-WANゾーン）に置き換える必要があります。
例えば、以前のポリシーで内部ネットワークからwan1へのトラフィックを許可していた場合、そのポリシーを更新して送信インターフェースをSD-WANに変更す

る必要があります。これにより、SD-WANエンジンがトラフィックを引き継ぎ、独自のルーティングルールを適用できるようになります。
最新ツール：従来は完全に手動で行っていたこの作業ですが、FortiOS 7.xにはインターフェース移行ウィザード（ネットワーク > インターフェース）が搭載されています。このツールは「検索と置換」機能を自動化し、既存のポリシーとルーティング参照を物理ポートからSD-WANオブジェクトに移動することで、ダウンタイムを最小限に抑えます。
他の選択肢が間違っている理由：
オプションB：ルーティングの更新（例えば、SD-WANインターフェースを指す0.0.0.0/0の静的ルートの作成）は必要ですが、カリキュラムでは、ファイアウォールポリシー内の参照の置き換えが主な管理上のハードルとして特に強調されています。これは、ポリシーがSD-WANに必要な単一の静的ルートよりも多く、複雑であることが多いためです。
オプションC：インターフェースを無効にする必要はありません。インターフェースは起動して設定済みである必要がありますが、他の設定参照から削除することで、SD-WANバンドルに「統合」できます。
オプションD：SD-WANはFortiOSの基本機能であり、有効化するために別途ライセンスや再起動は必要ありません。

有効的な**NSE5_SSE_AD-7.6**問題集はJPNTest.com提供され、**NSE5_SSE_AD-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE5_SSE_AD-7.6**試験問題集を提供します。JPNTest.com NSE5_SSE_AD-7.6試験問題集はもう更新されました。ここで**NSE5_SSE_AD-7.6**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/NSE5_SSE_AD-7.6-mondaishu **50**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 47
FortiGateでSD-WANルールを使用してローカルから送信へのpingトラフィックを制御したいと考えています。考慮すべき制約はどれですか？（2つ選択してください。）
A. SD-WANを使用するには、各ローカル出力機能を個別に設定する必要があります。
B. デフォルトでは、FortiGate は ping および traceroute に対応するローカルアウト トラフィックに対してのみ SD-WAN ルールを使用します。
C. 手動戦略を使用する SD-WAN ルールでのみ、ローカルから送信へのトラフィックを制御できます。
D. デフォルトでは、FortiGate は ping および traceroute に対応するローカルアウト トラフィックに対してのみ SD-WAN ルールを使用します。
正解: **A,B (**コメントを発表する**)**
SD-WAN 7.6 コア管理者カリキュラムでは、「ローカルアウト」トラフィック（DNS クエリ、FortiGuard アップデート、診断ピングなど、FortiGate 自体によって生成されるトラフィック）のルーティングには、このトラフィックが「フォワード」トラフィックとは異なるパスをたどるため、特別な設定が必要です。
* 個別設定（オプション A）：デフォルトでは、ローカルアウトトラフィックは SD-WAN エンジンをバイパスし、標準のシステムルーティングテーブル（RIB/FIB）を使用します。DNS や RADIUS などの特定の機能に SD-WAN ルールを使用するには、その機能の設定内で sdwan interface-select-method を個別に有効にする必要があります（例：config system dns または config user radius）。
* デフォルトのステアラブルトラフィック（オプション B）：FortiOS 7.6 では、ほとんどのローカルアウトトラフィックはデフォルトで SD-WAN から除外されますが、SD-WAN がアクティブな場合、特定の診断ローカルアウトトラフィック（具体的には ping と traceroute）に対して SD-WAN ルールを優先的に考慮し、管理者がユーザートラフィックと同じロジックを使用してパスの品質を確認できるように設計されています。
他の選択肢が間違っている理由：
* オプション C: interface-selection-method が sdwan に設定されている場合、ローカルアウト トラフィックは任意の SD-WAN 戦略 (手動、最高品質など) を使用してルーティングできます。

質問: 48

FortiSASEは、場所を選ばずに働く環境における3つの課題のうち、どれに対応していますか？ 3つ選択してください。）
A. セキュリティレベルの一貫性の欠如
B. 帯域幅不足
C. 可視性と制御の欠如
D. パフォーマンスが低い
E. リモートインターネット接続
正解: **(**正解を表示します**)**
文書化された 3 つのリモート ワークの課題は、一貫性のないセキュリティ、可視性と制御の欠如、パフォーマンスの問題です。Fortinet は、ユーザーは場所や信頼コンテキストによって異なるレベルの保護を受ける可能性があり、一貫性のないセキュリティの適用が生じると説明しています。従来のアーキテクチャでは、リモート アクセスされた SaaS トラフィックと企業データに対する可視性が制限され、セキュリティの盲点が生じます。FortiSASE_25_Administrator_Stud... パフォーマンスも課題です。従来のリモート アクセス設計では、インターネットと SaaS トラフィックを企業の VPN インフラストラクチャ経由でバックホールすることが一般的であり、遅延が発生し、ユーザー エクスペリエンスが低下する可能性があります。
FortiSASE_25_Administrator_Stud... FortiSASE は、一貫したクラウドベースのセキュリティ検査、一元化された可視性とポリシーの適用、分散した場所からの最適化されたアクセスを提供することで、これらの問題に対処します。生の帯域幅の不足やリモートのインターネット接続の不足自体は、FortiSASE コースの教材で特定された 3 つのアーキテクチャ上の課題ではありません。

有効的な**NSE5_SSE_AD-7.6**問題集はJPNTest.com提供され、**NSE5_SSE_AD-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE5_SSE_AD-7.6**試験問題集を提供します。JPNTest.com NSE5_SSE_AD-7.6試験問題集はもう更新されました。ここで**NSE5_SSE_AD-7.6**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/NSE5_SSE_AD-7.6-mondaishu **50**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」