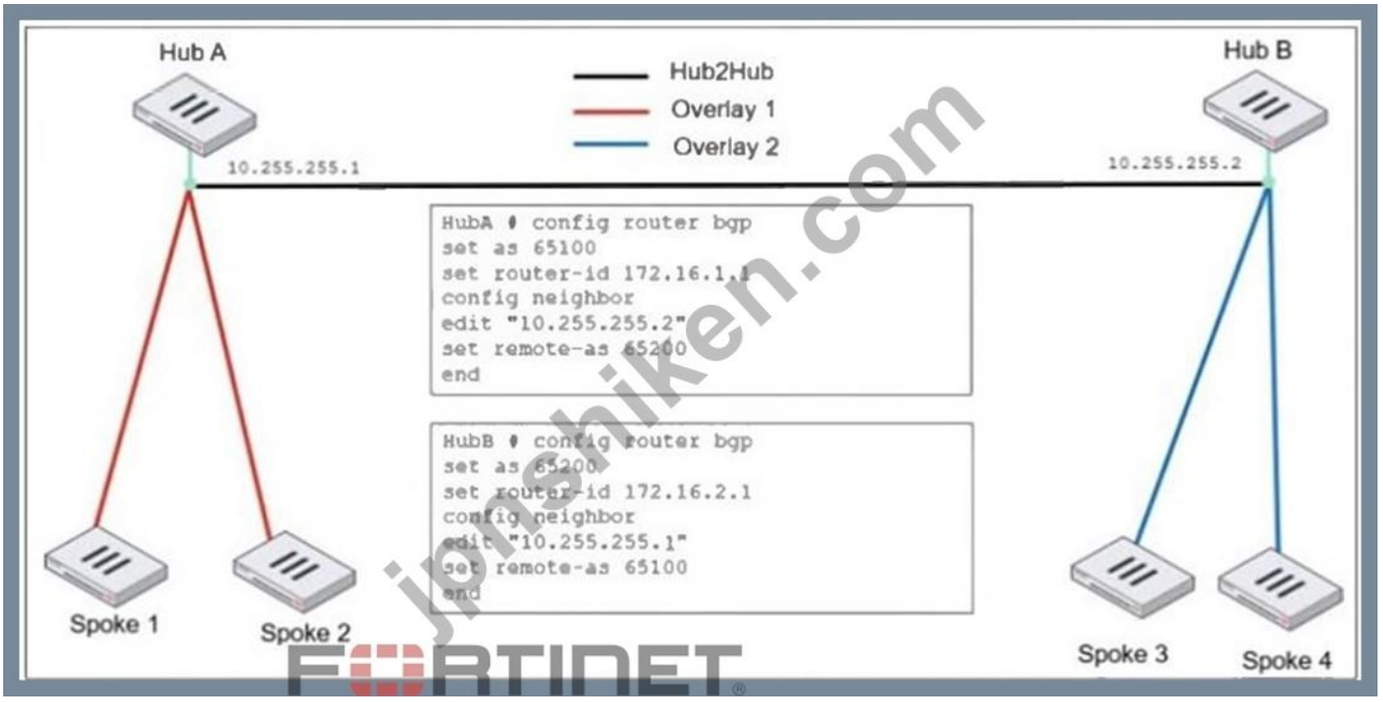
Fortinet.FCSS_EFW_AD-7.6.v2026-03-23.q25

試験コード：	FCSS_EFW_AD-7.6
試験名称：	FCSS - Enterprise Firewall 7.6 Administrator
認証ベンダー：	Fortinet
無料問題の数：	25
バージョン：	v2026-03-23
ページの閲覧量：	104
問題集の閲覧量：	251

https://www.jpnshiken.com/shiken/Fortinet.FCSS_EFW_AD-7.6.v2026-03-23.q25.html

質問: **1**

ADVPNネットワークを示す展示を参照してください



管理者は、オーバーレイ ネットワーク 1 と 2 を接続するために、IBGP と EBGP を使用して ADVPN を構成する必要があります。

管理者が BGP で設定する必要がある 2 つのオプションは何ですか? (2 つ選択してください。)

A. ebgp-enforce-multirhop を有効にする

B. next-hop-self を有効にする

C. ibgp-enforce-multihop advpn を設定する

D. 属性変更なしのネクストホップを設定する

正解: **(正解を表示します)**

このADVPN（自動検出VPN）ネットワークでは、2つのハブ（ハブAとハブB）がEBGPで接続されており、各オーバーレイ内ではIBGPが使用されています。オーバーレイ間のBGPルーティングを適切に行うには、管理者が特定のBGPオプションを設定する必要があります。

ebgp-enforce-multihop を有効にする

デフォルトでは、EBGPは直接接続されたネイバーを必要とします。ハブAとハブBは直接接続されておらず、IPsecトンネルを介して相互にアクセスしているため、EBGPセッションが機能するにはマルチホップを有効にする必要があります。
ネクストホップセルフを有効にする
IBGPでは、ネクストホップ属性はデフォルトでは変更されません。IBGPルートがスポークから別のハブまたはスポークにアドバタイズされる場合、適切な到達可能性を確保するためにネクストホップを更新する必要があります。next-hop-selfを有効にすると、BGPスピーカーは自身をネクストホップとしてアドバタイズするように強制され、すべてのスポークがオーバーレイを介したルートに適切に到達できるようになります。

質問: **2**
管理者は ADVPN 構成を設定しており、VPN の確立中にピア ID が公開されないようにしたいと考えています。
管理者はセキュリティを強化するためにどのプロトコルを使用できますか?
A. ピア ID を暗号化して漏洩を防ぐ IKEv2 を使用します。
B. ピア ID をまったく使用しないため、SSL VPN Web モードを選択します。
C. ピアの識別を簡素化するため、IKEv1 アグレッシブ モードを選択します。
D. パフォーマンスが向上するため、IKEv1 メイン モードを使用します。
正解: **(**正解を表示します**)**
ADVPN（自動検出VPN）構成では、VPN確立時のピアIDの保護がセキュリティ上の懸念事項となります。ピアIDはIKE（インターネット鍵交換）ネゴシエーションフェーズで交換されるため、その漏洩はプライバシーリスクや標的型攻撃につながる可能性があります。
IKEv2 はピア ID を暗号化するため、アグレッシブ モードでピア ID をプレーンテキストで公開できる IKEv1 と比較して、より安全です。
IKEv2 は、ADVPN での動的なトンネルの確立をサポートしながら、より優れたパフォーマンスと柔軟性も提供します。

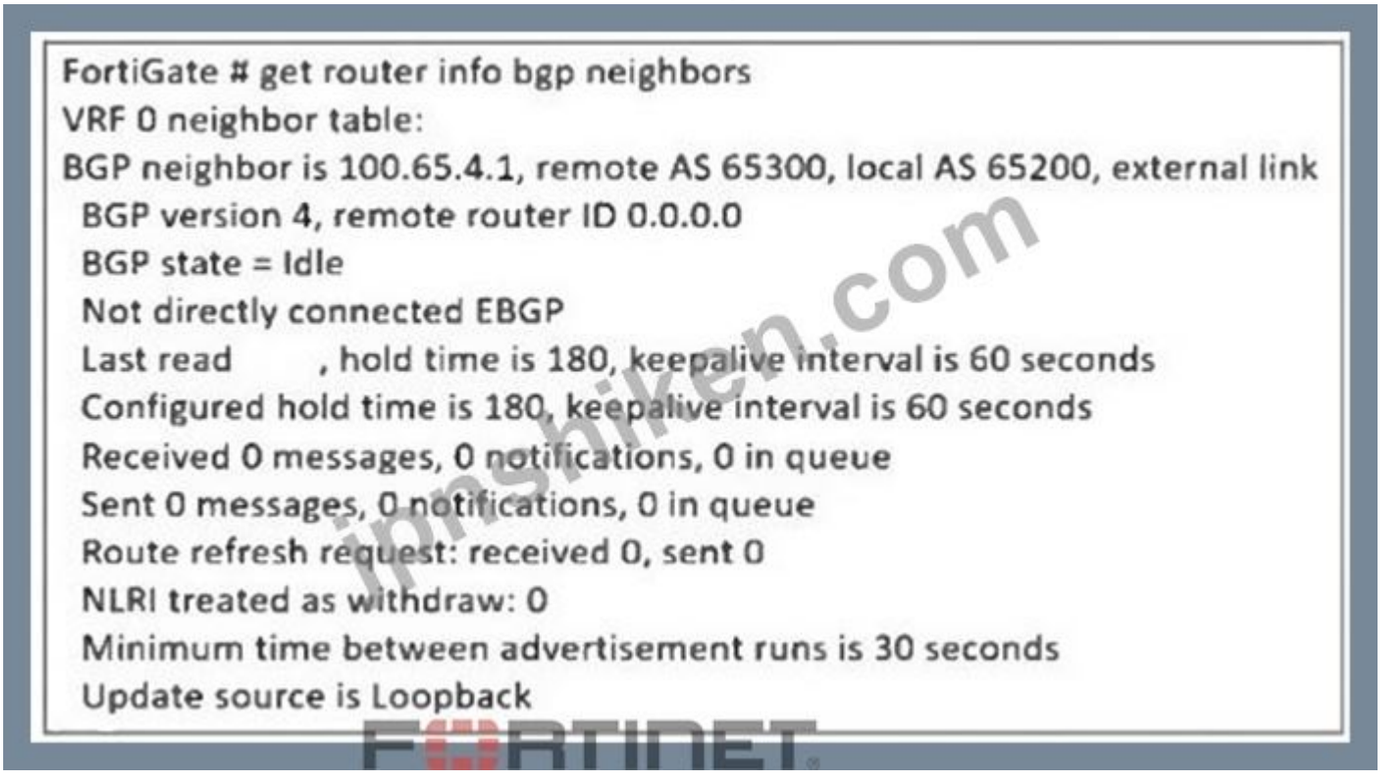
質問: **3**
企業のネットワーク トラフィックを保護するために、セッションの最初のパケットを処理するときに、FortiGate は最初にどのステップを実行しますか? (回答を 1 つ選択してください)
A. ネットワークプロセッサ（NP）へのセッションキーのインストール
B. 復号化
C. 逆パス転送（RPF）チェック
D. IP整合性ヘッダーのチェック
正解: **D (**コメントを発表する**)**
包括的かつ詳細な 150 ～ 200 語の説明 (Enterprise Firewall 7.6 管理者ドキュメントの完全な抜粋より):

FortiOS 7.6管理ガイドおよび「Life of a Packet」ドキュメント（並列パス処理）に基づき、FortiGateは新しいセッションの最初のパケットを処理する際に、特定のハードコードされたシーケンスに従います。このプロセスは、入力、カーネル、出力という複数のステージに分かれています。
最初の段階はイングレスです。ここでは、ネットワークインターフェースが受け入れたすべてのパケットがTCP/IPスタックによって処理されます。この直後、パケットはIP整合性ヘッダーチェックを通過する必要があります。このステップでは、パケットヘッダーを読み取り、パケットが有効なプロトコル（TCP、UDP、ICMPなど）であり、ヘッダー長が正しいことを確認します。この整合性チェックは、復号化（イングレス段階の後半で実行）やリバースパスフォワーディング（RPF）チェック（カーネル段階のルーティング段階でさらに後半で実行）などの他のセキュリティ機能よりも先に実行されます。
セッションキーのインストール（オプションA）は、パケットがファイアウォールポリシーに一致し、セッションが完全に確立されてNPUにオフロードされた後にのみ行われます。したがって、IP整合性ヘッダーのチェックは、受信パケットに対して実行されるセキュリティ関連の検証の中で、最も最初に実行されるものとなります。

質問: **4**
管理者は、FortiGate ファイアウォールでの CPU と RAM の使用を最小限に抑えながら、Web フィルタリングや HTTPS トラフィックのアプリケーション制御などの重要なセキュリティ機能も有効にする必要があります。
暗号化された HTTPS トラフィックの Web フィルタリングやアプリケーション制御などのセキュリティ機能を有効にしながら、システム負荷を軽減するのに役立つ SSL 検査設定はどれですか。
A. 完全な SSL 検査を使用して、暗号化されたペイロードを徹底的に検査します。
B. リソースを節約するために SSL 検査を完全に無効にします。
C. HTTPS トラフィックを効率的に処理するために SSL 検査を構成します。
D. SSL 証明書検査モードを有効にして、トラフィックを復号化せずに基本的なチェックを実行します。
正解: **(正解を表示します)**
Web フィルタリングやアプリケーション制御などのセキュリティ機能を適用しながら CPU と RAM の使用を最小限に抑えるには、SSL 証明書検査モードが最適です。
SSL 証明書検査により、FortiGate は暗号化されたペイロード全体を復号化せずに、サーバー名表示 (SNI) と証明書の詳細を含む SSL/TLS ハンドシェイクのみを検査できます。
これにより、FortiGate は SNI と証明書情報に基づいて宛先の Web サイトまたはアプリケーションを判別できるため、Web フィルタリングやアプリケーション制御などの機能が有効になります。
トラフィックの完全な復号化と再暗号化を必要とする完全な SSL 検査と比較して、システム負荷が大幅に軽減されます。

質問: **5**

コマンド出力の一部を含む展示を参照してください。



管理者はFortiGateにBGPを設定しました。この新しいBGP設定のステータスは図に示されています。

管理者は次にどのような構成を考慮する必要がありますか?

A. 100.65.4.1 への静的ルートを設定します。

B. ローカル AS を 65300 に設定します。

C. リモートピア管理者に連絡してBGPを有効にしてください

D. ebgp-enforce-multihop を有効にします。

正解: **(**正解を表示します**)**

BGP ネイバー ステータス出力から、重要な問題は BGP が 「アイドル」状態のままになっていることです。つまり、FortiGate はピア 100.65.4.1 (リモート AS 65300) との BGP セッションを確立できません。

出力には次の内容も表示されます。

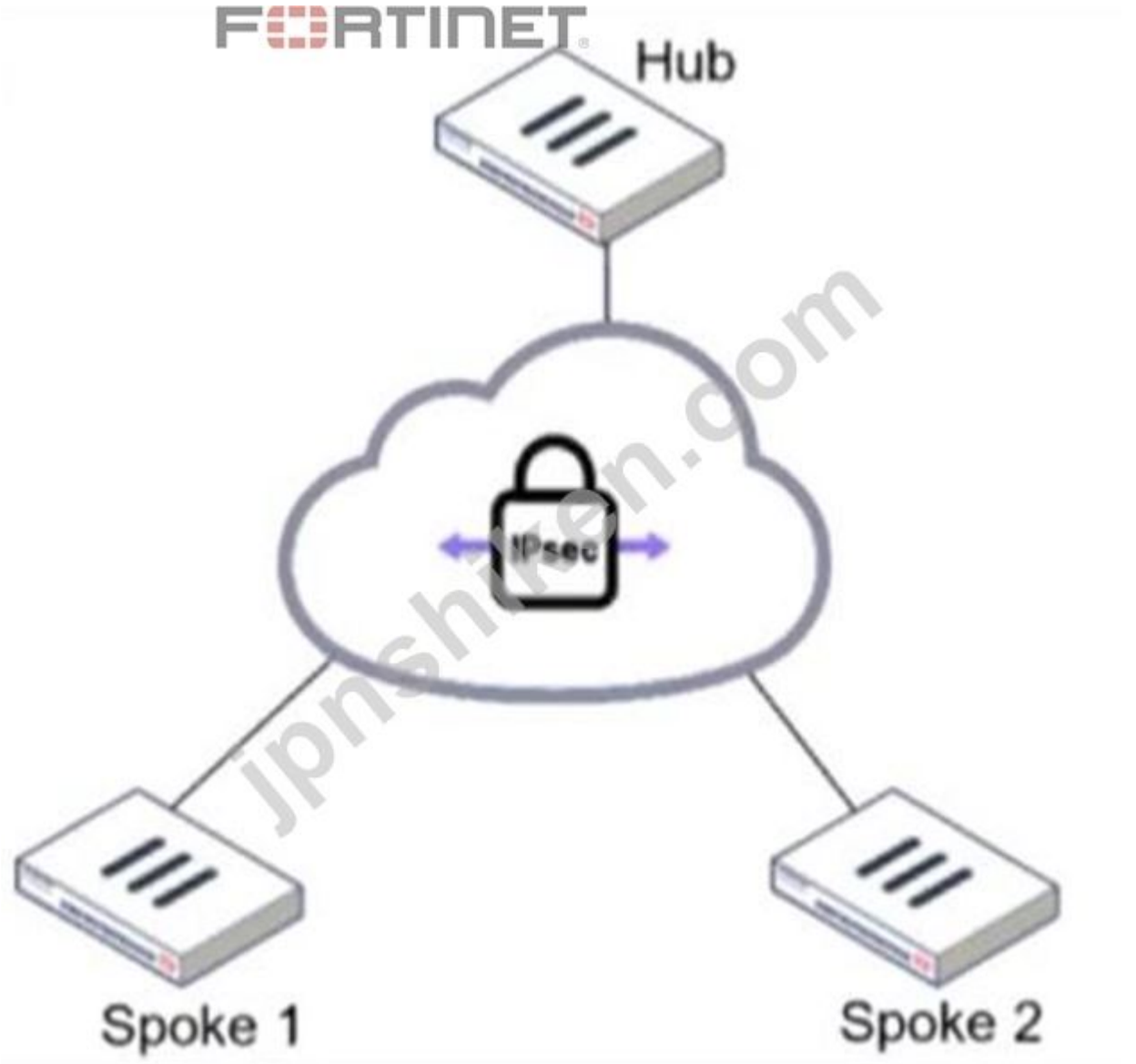
EBGP に直接接続されていません」# これは、BGP ピアが同じサブネット上になく、マルチホップ BGP が必要であることを意味します。

更新ソースはループバックです」# ループバック インターフェイスが使用されるため、複数ホップ上の BGP ネイバーを許可するように FortiGate を設定する必要があります。

この問題を解決するには、管理者は ebgp-enforce-multihop を有効にする必要があります。これにより、ネイバーが直接接続されていない場合でも BGP セッションを確立できるようになります。

質問: **6**

展示品を参照してください。



管理者はハブ アンド スポーク ネットワークを展開し、OSPF を動的プロトコルとして使用しています。
ネイバー隣接関係に必須な設定はどれですか?
A. ルータ設定でBFDを有効にする
B. ハブインターフェースのネットワークタイプをポイントツーマルチポイントに設定する
C. ルータの設定で rfc1583 互換を有効にする
D. ハブインターフェースで仮想リンクを有効にする
正解: **(**正解を表示します**)**
IPsec VPN 上で OSPF を使用するハブアンドスポークトポロジでは、ハブとスポーク間のネイバー隣接関係を確立するために、ポイントツーマルチポイントネットワークタイプが必要です。このネットワークタイプにより、指定ルータ (DR) を必要とせずに OSPF が正しく動作し、IPsec トンネルを介した動的なルーティング更新が可能になります。

質問: **7**

FortiGateではVirtual eXtensible LAN（VXLAN）を多用されています。FortiGateのパフォーマンスを向上させるには、どのような専用のアクセラレーションハードウェアを使用する必要がありますか？（1つ選択してください）

A. NP7

B. SP5

C. ##9

D. NTurbo

正解: **A (**コメントを発表する**)**

包括的かつ詳細な 150 ～ 200 語の説明 (Enterprise Firewall 7.6 管理者ドキュメントの完全な抜粋より):

FortiOS 7.6インフラストラクチャ学習ガイドとハードウェアアクセラレーションに関するドキュメントによると、ネットワークプロセッサ7（NP7）は、システムCPUから高性能ネットワークトラフィックをオフロードするために設計されたフラッグシップハードウェアコンポーネントです。NP7が以前の世代（NP6など）と比べて大きく進化した点は、Virtual eXtensible LAN（VXLAN）ハードウェアアクセラレーションをネイティブにサポートしていることです。

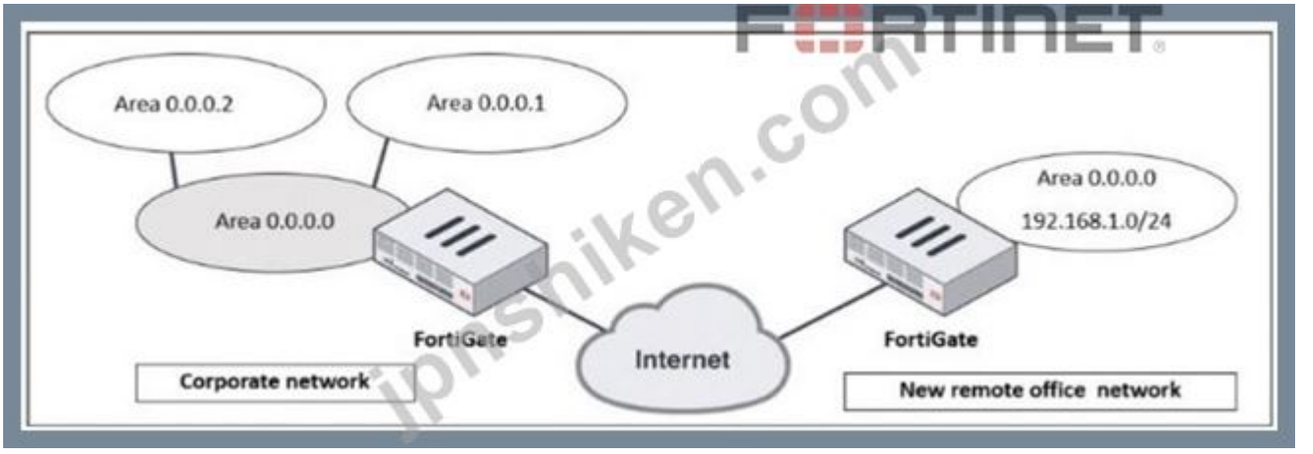
VXLANを用いてレイヤ2セグメントをレイヤ3ネットワーク上に拡張するエンタープライズ環境では、VXLANヘッダーのカプセル化とデカプセル化の計算コストが高くなる可能性があります。NP7は、これらの処理をラインレートで実行するための専用回路を備えており、レイテンシを大幅に低減し、CPUの飽和を防ぎます。これにより、FortiGateは複雑なオーバーレイトンネルを処理する場合でも高いスループットを維持できます。

CP9（コンテンツプロセッサ）（オプションC）はSSL/TLSインスペクションとIPsec暗号化の高速化を提供しますが、VXLANのようなネットワーク層のカプセル化は処理しません。NTurbo（オプションD）は、ファイアウォールセッションをネットワークプロセッサにオフロードするソフトウェア機能であり、ハードウェアチップではありません。SP5（オプションB）も新しいミッドレンジモデルでVXLANオフロードをサポートしていますが、NP7が主な機能です。

7.6 カリキュラムでハイエンドのエンタープライズ パフォーマンスを実現するために参照される「特殊なアクセラレーション ハードウェア」。

質問: **8**

企業ネットワークと新しいリモート オフィス ネットワークを示す展示を参照してください。



管理者は、新しいリモート オフィス ネットワークを企業のエンタープライズ ネットワークと統合する必要があります。
2 つのネットワーク間のルーティングを可能にするために管理者は何をする必要がありますか?
A. 管理者は、新しいリモートオフィスネットワークを企業のFortiGateデバイスに組み込むためにBGPを実装する必要があります。
B. 管理者は、企業の FortiGate デバイス上のサブネット 192.168.l.0/24 への静的ルートを設定する必要があります。
C. 管理者は両方の FortiGate デバイスで仮想リンクを設定する必要があります。
D. 管理者は、両方の FortiGate デバイスに OSPF over IPsec を実装する必要があります。
正解**: (**正解を表示します**)**
このシナリオでは、企業ネットワークと新しいリモートオフィスネットワークはインターネットを介して通信する必要があり、安全で動的なルーティング方式が必要です。両方のネットワークはルーティングプロトコルとしてOSPF（Open Shortest Path First）を使用しているため、安全で動的なルート伝播を確保するために、OSPF over IPsec VPNを構築するのが最適なアプローチです。
企業ネットワークでは既にOSPFが稼働しており、これをIPsecトンネル上に拡張することで、企業のFortiGateとリモートオフィスのFortiGate間で動的なルート交換が可能になります。IPsecはインターネット経由のトラフィックを暗号化し、安全な通信を保証します。OSPF over IPsecにより、手動での静的ルート設定が不要になり、ネットワークが変更されてもルートが自動的に更新されます。
新しいリモート オフィスの 192.168.1.0/24 サブネットは、追加の構成なしで企業ネットワークに動的にアドバタイズされます。

質問**: 9**
ユーザーは、セキュリティで保護された HTTPS ウェブサイトにアクセスした後にコンピュータがマルウェアに感染したと報告しました。
しかし、管理者が FortiGate ログを確認すると、SSL 証明書があり、ポリシーに正しいプロファイルが適用されているにもかかわらず、Web サイトが安全でないと検出されたことがわかりません。
管理者はどのようにして、FortiGate が Web サイト上の暗号化された HTTPS トラフィックを分析できることを確認できますか?
A. 管理者は、信頼できる Web サイトを有効にして、FortiGuard Web フィルターによって評価された SSL/TLS Web サイトのみを許可する必要があります。
B. 管理者は、TLS 3 ウェイ ハンドシェイクが FortiGate によって正しく分析されるように、SSL 証明書検査で SNI からの URL 抽出を有効にする必要があります。
C. 管理者は、HTTPS ウェブサイト上の一般的な DNS 要求で分析できない偽の Server Name Indication (SNI) から保護するために、DNS over TLS を有効にする必要があります。
D. 管理者は、パケットを復号化し、期待どおりに分析されるようにするために、SSL/SSH 検査プロファイルで完全な SSL 検査を有効にする必要があります。

正解: **D** (コメントを発表する)
FortiGateは、他のセキュリティアプライアンスと同様に、暗号化されたHTTPSトラフィックを事前に復号化しない限り、分析できません。証明書検査のみが有効になっている場合、FortiGateは証明書の詳細（ドメインや発行者など）を確認できますが、実際のWebコンテンツを検査することはできません。
トラフィックを完全に分析し、潜在的なマルウェアの脅威を検出するには:
SSL/SSH 検査プロファイルで完全な SSL 検査 (ディープ パケット インスペクション) を有効にする必要があります。
これにより、FortiGate は HTTPS トラフィックを復号化し、コンテンツを検査し、ユーザーに転送する前に再暗号化できるようになります。
完全な SSL 検査がないと、暗号化されたトラフィックに埋め込まれた脅威が検出されない可能性があります。

質問: **10**
物理トポロジとトラフィック ログを示す展示を参照してください。

管理者は、FortiGate ISFW デバイスの背後にある IP アドレス 10.1.10.1 のデバイスからの FortiAnalyzer トラフィックをチェックしています。
ISFW デバイスのファイアウォール ポリシーでは UTM が有効になっていないため、図に示すように、管理者はマルウェア アクションのログを見て驚きます。
FortiAnalyzer がこのログを表示する 2 つの理由は何ですか? (2 つ選択してください。)
A. ISFW でセキュリティ評価が有効になっています。
B. ISFW は Security Fabric 環境内にあります。
C. ISFW は FortiAnalyzer に接続されていないため、NGFW-1 を経由する必要があります。
D. NGFW-1 のファイアウォール ポリシーで UTM が有効になっています。
正解: (正解を表示します)
展示によると、ISFWはNGFW-1をファブリックルートとするセキュリティファブリック環境の一部です。このアーキテクチャでは、FortiGateデバイスはログや検出された脅威などのセキュリティインテリジェンスを共有します。
ISFW は Security Fabric 環境内にあります:
Security Fabric を使用すると、UTM がローカルで有効になっていない場合でも、ISFW などのデバイスが NGFW-1 から脅威インテリジェンスを受信できるようになります。

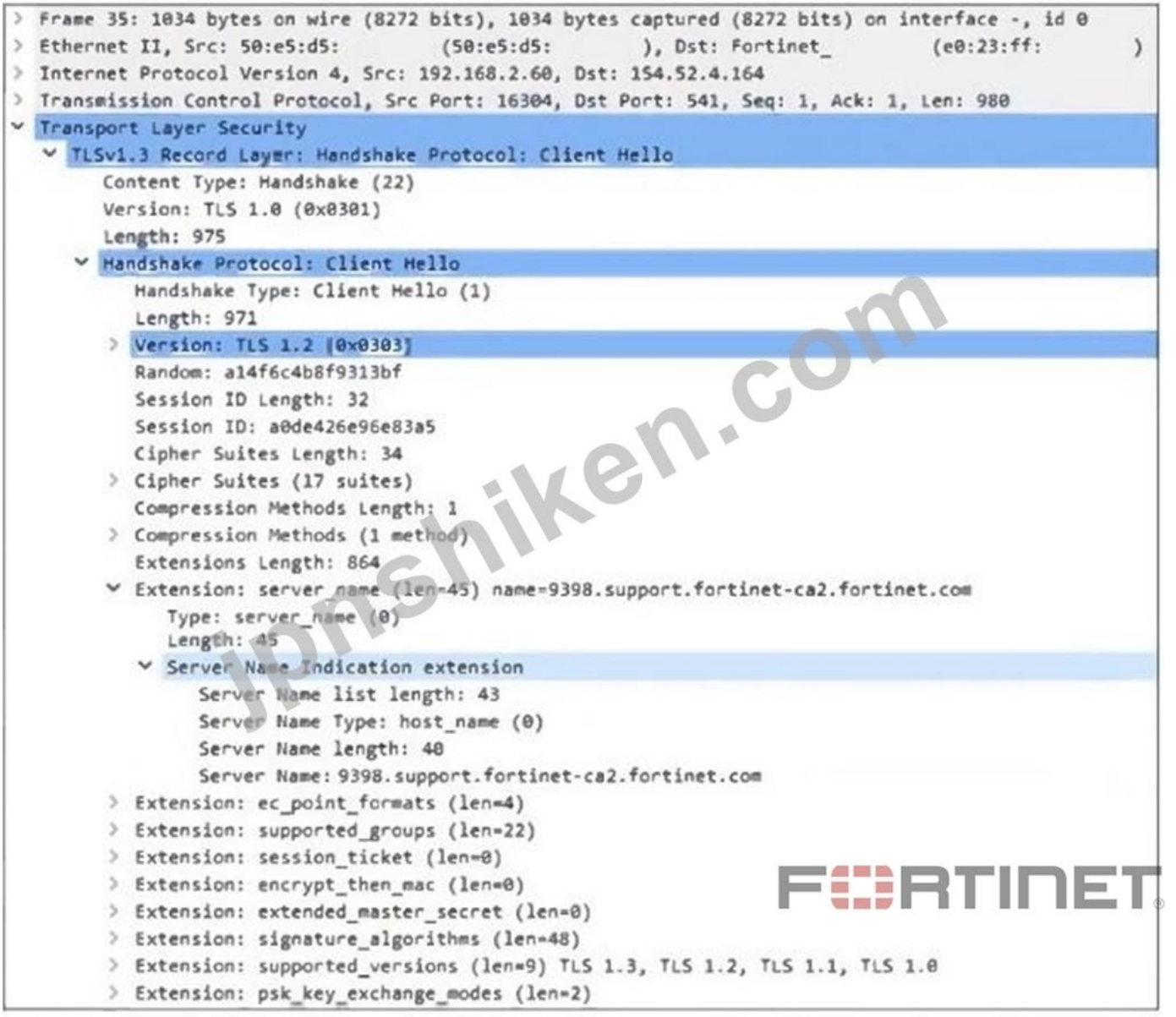
NGFW-1 が IP 10.1.10.1 から 89.238.73.97 までのマルウェアを検出すると、この情報は ISFW および FortiAnalyzer に伝播される可能性があります。
NGFW-1 のファイアウォール ポリシーでは UTM が有効になっています。
ISFW では UTM が有効になっていませんが、NGFW-1 (ISFW と外部ネットワークの間にある) では UTM が有効になっていて、トラフィックをスキャンしています。
NGFW-1 はセッションでマルウェアを検出すると、イベントをログに記録し、FortiAnalyzer に送信します。

質問: **11**
複数の国にまたがる複数の支店を買収した企業は、各支店に新しいFortiGateデバイスを導入する必要があります。しかし、ITスタッフにはFortiGateデバイスの初期設定を行うための十分な知識が不足しています。
リモート ブランチに高度な初期構成を正常に展開するために、企業が実行できる 3 つのアプローチはどれですか。(3 つ選択してください。)
A. メタデータ変数を使用して、各 FortiGate デバイスに応じて値を動的に割り当てます。
B. プロビジョニング テンプレートを使用し、デバイス レイヤーで構成設定をインストールします。
C. グローバル ADOM を使用して、グローバル オブジェクト構成を各 FortiGate デバイスに展開します。
D. 大規模かつ高度な導入のために、FortiManager スクリプトに Jinja を適用します。
E. FortiManager に FortiGate デバイスをモデル デバイスとして追加し、ZTP または LTP を使用して FortiGate デバイスに接続します。
正解: **(正解を表示します)**
メタデータ変数を使用して、各 FortiGate デバイスに応じて値を動的に割り当てます。
FortiManagerのメタデータ変数を使用すると、各FortiGateを手動で設定することなく、デバイス固有の設定を動的に割り当てることができます。これは、類似した基本設定を持つ複数のデバイスを導入する場合に特に便利です。
プロビジョニング テンプレートを使用して、デバイス レイヤーで構成設定をインストールします。
FortiManagerのプロビジョニングテンプレートは、FortiGateデバイスを構造的に構成する方法を提供します。これらのテンプレートでは、インターフェース、ポリシー、および設定を定義できるため、導入時に各デバイスが正しく構成されることを保証します。
FortiManager に FortiGate デバイスをモデル デバイスとして追加し、ZTP または LTP を使用して FortiGate デバイスに接続します。
ゼロタッチプロビジョニング（ZTP）とローカルタッチプロビジョニング（LTP）は、FortiGateデバイスの導入を自動化します。FortiManagerでデバイスをモデルデバイスとして追加することで、デバイスの初回接続時に設定が自動的にプッシュされ、手作業の負担を軽減します。

質問: **12**

FortiGate と FortiManager Cloud 間の 3 ウェイ ハンドシェイクのパケット キャプチャ出力を示す図を参照してください。

Packet capture output of three-way handshake between a FortiGate and a FortiManager Cloud



この展示からどのような 2 つの結論を引き出すことができますか? (2 つ選択してください。)

A. FortiManager はクラウド コンピューティング環境で動作するため、FortiGate は複数のドメインをサポートする証明書を受け取ります。

B. FortiGate は同じ IP サーバーに接続しており、FortiGate と FortiManager Cloud 間の接続用に独立した証明書を受け取ります。

C. TLS ハンドシェイクに 17 個の暗号スイートが含まれている場合、この 3 ウェイ ハンドシェイクの TLS バージョンは 1.0 である必要があります。

D. ドメイン *.fortinet-ca2.support.fortinet.com のワイルドカードは、FortiManager Cloud でサポートされている必要があります。

正解: (正解を表示します)

パケットキャプチャの出力には、FortiGateからFortiManager CloudへのTLS Client Helloメッセージが表示されます。このメッセージには、FortiGateが接続しようとしているドメイン名を示すために使用されるServer Name Indication（SNI）が含まれています。
FortiManager はクラウド コンピューティング環境で動作するため、FortiGate は複数のドメインをサポートする証明書を受け取ります。
FortiManager Cloud は、共有インフラストラクチャの下で複数の顧客とドメインをホストします。
TLS ハンドシェイクには SNI (Server Name Indication) が含まれており、これにより FortiManager Cloud は要求されたドメインに基づいて複数の証明書を提供できるようになります。
これは、FortiGate が FortiManager Cloud の下で複数の顧客に使用できるマルチドメイン証明書またはワイルドカード証明書を受け取る可能性が高いことを意味します。
ドメイン .fortinet-ca2.support.fortinet.com のワイルドカードは、FortiManager Cloud でサポートされている必要があります。
SNI 拡張機能には、ドメイン 9398.support.fortinet-ca2.fortinet.com が含まれています。
FortiManager Cloud は、複数のサブドメインと顧客を安全に管理するために、*.fortinet-ca2.support.fortinet.com などのワイルドカード証明書をサポートする必要があります。
これにより、FortiGate は TLS エラーなしでサーバー証明書を検証できるようになります。

質問: **13**
管理者が VPN トポロジに IKEv2 を実装することを決定した場合、IKEv2 に関する次の 2 つの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. 楕円曲線 (ECP) グループなどのより強力な Diffie-Hellman (DH) グループが含まれます。
B. IKEv1 を使用するデバイスとの相互運用性をサポートします。
C. 安全なトンネルを確立するために、少なくとも 2 つのメッセージを交換します。
D. 拡張認証プロトコル (EAP) をサポートします。
正解: **(**正解を表示します**)**
IKEv2 (インターネット キー エクスチェンジ バージョン 2) は IKEv1 を改良したもので、VPN 構成のセキュリティ、効率、柔軟性が向上しています。
これには、楕円曲線 (ECP) グループなどの強力な Diffie-Hellman (DH) グループが含まれます。
IKEv2 は、ECP256 や ECP384 などの楕円曲線 Diffie-Hellman (ECDH) グループを含む強力な暗号化アルゴリズムをサポートし、IKEv1 と比較してセキュリティが向上しています。
拡張認証プロトコル (EAP) をサポートしています。
IKEv2はEAP認証をネイティブにサポートしており、RADIUS、証明書、スマートカードなどの外部認証メカニズムとの統合が可能です。これは、ユーザー認証の柔軟性とセキュリティが求められるリモートアクセスVPNに特に役立ちます。

質問: **14**
コマンド出力を示す展示を参照してください。

FortiGate_A と FortiGate_B は、エンタープライズ ネットワーク内の FGSP クラスターのメンバーです。
管理者は、ping コマンドを使用してクラスターをテストしているときにパケット損失を監視し、FortiGate_B のセッション出力が図のとおりであることを発見しました。
FortiGate_B のこの出力の原因は何でしょうか?

A. セッション同期は暗号化されます。
B. FortiGate_B で session-pickup-connectionless が無効に設定されています。
C. FortiGate_B はパッシブ モードに設定されています。
D. FortiGate_A と FortiGate_B は同じ standalone-group-id 値を持ちます。
正解: **(**正解を表示します**)**
Fortinet FGSP（FortiGate Session Life Support Protocol）クラスタは、2台のFortiGateデバイス間のセッション同期を可能にし、シームレスなフェイルオーバーを実現します。ただし、ICMP（ping）はコネクションレス型プロトコルであるため、FortiGateは明示的に有効にしない限り、デフォルトではコネクションレス型セッションを同期しません。
展示内容：
FortiGate_B でコマンド get system session list | grep icmp を実行しても出力が返されません。これは、ICMP セッションが FortiGate_A から同期されていないことを意味します。
session-pickup-connectionless が無効になっている場合、FortiGate_B は ICMP セッションを受信せず、フェイルオーバー中にパケット損失が発生します。

質問: **15**
ネットワーク伝送パターンとアプリケーション シグネチャに重点を置いて、IPS プロトコル デコーダーを使用してトラフィックをブロックするには、FortiGate でどのようなアクションを実行できますか?

A. DNS フィルターを使用して、アプリケーション署名とプロトコル デコーダーをブロックします。
B. アプリケーション制御を使用して、URL ベース以外のソフトウェアの処理を制限します。
C. アプリケーション検出ベースの SD-WAN ルールを有効にします。
D. フロー モードで Web フィルタ プロファイルを構成します。
正解: **(**正解を表示します**)**
FortiGateのIPSプロトコルデコーダーは、ネットワーク伝送パターンとアプリケーションシグネチャを分析し、悪意のあるトラフィックを識別してブロックします。アプリケーション制御機能は、従来のURLに依存しないアプリケーションであっても、その動作とシグネチャに基づいてFortiGateがアプリケーションを検出、分類、ブロックすることを可能にします。

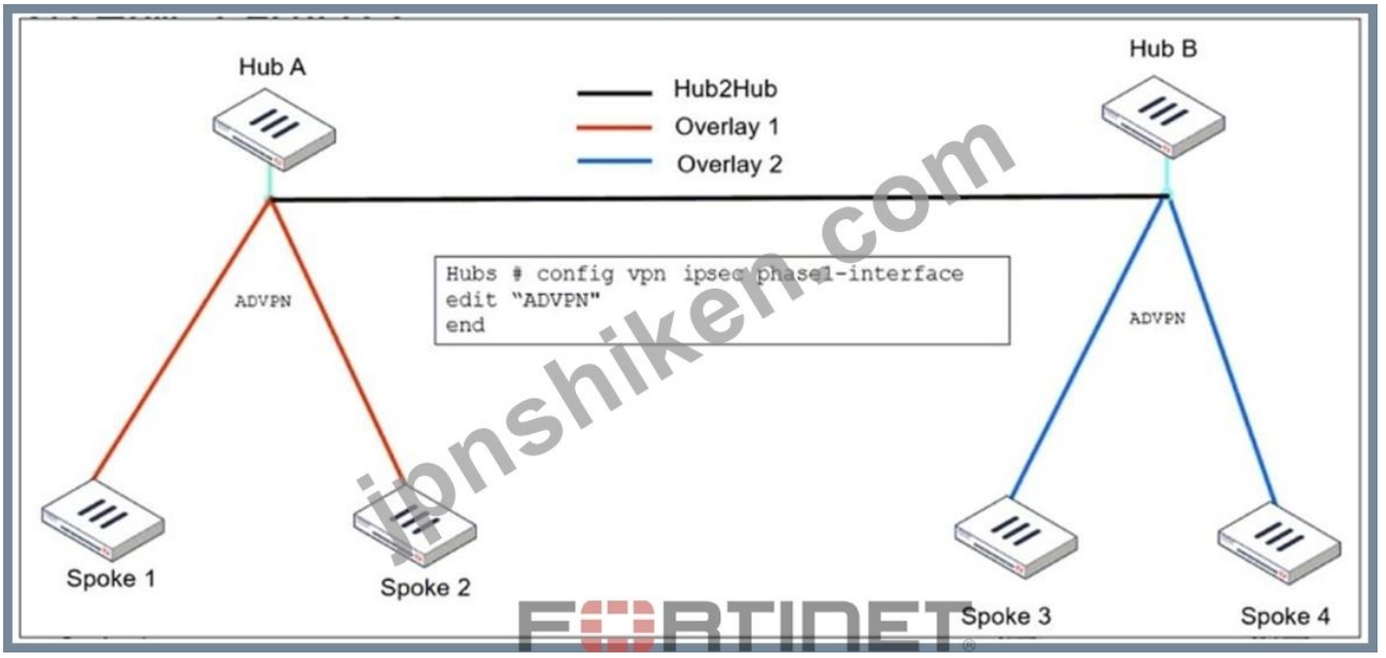
アプリケーション制御は IPS プロトコル デコーダーと連携してパケット ペイロードを検査し、認識されたアプリケーションの動作に基づいてセキュリティ ポリシーを適用します。
P2P トラフィック、VoIP、メッセージング アプリ、および IPS がプロトコル デコーダーを通じて識別できるその他の非 Web ベース プロトコルなどの非 URL ベース アプリケーションをきめ細かく制御できます。
IPS とアプリケーション制御を組み合わせることで、従来のファイアウォール ルールを回避する可能性のある、回避的なアプリケーションや暗号化されたアプリケーションを検出できます。

質問: **16**
透過的 VDOM インターフェイスのコマンド set forward-domain <domain_ID> は何をしますか?
A. ドメイン ID に基づいてトラフィックの優先順位を設定するようにインターフェイスを設定し、指定された VLAN のサービス品質を向上させます。
B. VLAN ID に基づいてインターフェースにブロードキャスト ドメインを割り当てることで、特定の VLAN 内のトラフィックを分離します。
C. 指定された VLAN からのトラフィックのみを管理するようにインターフェイスを制限し、ネットワーク トラフィックを効果的に分離します。
D. インターフェイスに一意のドメイン ID を割り当て、同じ VDOM 内の複数の VLAN にわたって動作できるようにします。
正解: **(**正解を表示します**)**
透過モードの仮想ドメイン（VDOM）構成では、FortiGateはレイヤ3ルーティングではなく、レイヤ2ブリッジとして動作します。set forward-domain <domain_ID>コマンドは、同じ透過VDOM内のインターフェース間でトラフィックを転送する方法を制御するために使用されます。
フォワードドメインはブロードキャストドメインとして機能します。つまり、同じフォワードドメインIDを持つインターフェースのみがトラフィックを交換できます。この設定は、FortiGateによるセキュリティポリシーの適用を可能にしながら、透過的なVDOM内で異なるVLANまたはネットワークセグメントを分離するためによく使用されます。

質問: **17**
管理者は、サーバーを保護するためにクライアントとサーバーのターゲットにブロックオールの IPS プロファイルを適用しましたが、データベース チームから、その直後にアプリケーションが動作しなくなったと報告されました。

管理者は、ネットワーク内の既存のアプリケーションを中断せずに IPS を適用するにはどうすればよいでしょうか?
A. すべてのシグネチャをモニター モードで含む IPS プロファイルを使用し、ブロックする前にパターンを検証します。
B. サーバーからクライアントへの接続がブロックされないように、IPS プロファイルをサーバーターゲットのみに制限します。
C. アプリケーション パターンを正確に分析するには、IPS プロファイルでフロー モードを選択します。
D. IPS プロファイル シグネチャ アクションをデフォルトに設定して、すべての誤検知の可能性を破棄します。
正解: **A (**コメントを発表する**)**
事前のテストなしにアグレッシブなIPSプロファイルを適用すると、通常のトラフィックを悪意のあるトラフィックと誤認し、正当なアプリケーションの動作を阻害する可能性があります。脅威を監視しつつ、動作の阻害を防ぐには、以下の手順を実行してください。
まず「モニターモード」でIPSを有効にします。
これにより、FortiGate はトラフィックを積極的にブロックすることなく、潜在的な脅威をログに記録して分析できます。
管理者は、ブロッキング モードに切り替える前にログを確認し、IPS シグネチャを微調整して誤検知を最小限に抑えることができます。
署名パターンを検証して調整します。
一部のシグネチャは、正当なアプリケーション トラフィックに対して不要なブロックをトリガーする可能性があります。
ログを分析することで、管理者は誤検知の原因となる特定のルールを無効化または変更できます。

質問: **18**
図を参照してください。これは、ハブ A からスポーク 1 およびスポーク 2、およびハブ # からスポーク 3 およびスポーク 4 までの VPN IPsec フェーズ 1 を表す ADVPN IPsec インターフェイスを示しています。



管理者は、オーバーレイ ネットワーク 1 と 2 を接続するために、IBGP と EBGP を使用して ADVPN を構成する必要があります。

管理者は、ADVPN トンネルのフェーズ 1 VPN IPsec 構成で何を構成する必要がありますか?

A. 自動検出送信者を有効にし、ネットワーク ID を x に設定する

B. auto-discovery-forwarder を有効にし、remote-as x を設定します。

C. auto-discovery-crossover を有効にし、enforce-multihop を有効にします。

D. 自動検出レシーバーを有効にし、npu-offload を有効にします

正解: **(**正解を表示します**)**

IBGP と EBGP を使用して異なるハブ間のオーバーレイ ネットワークを接続するように ADVPN (自動検出 VPN) を構成する場合、異なるオーバーレイ ネットワークのスポークが動的にトンネルを確立できるように特別な構成が必要です。

自動検出クロスオーバーを有効にする

これにより、複数のハブが使用される ADVPN 展開で、ハブ間のトンネル検出が可能になります。

ハブ A とハブ B は異なるオーバーレイに属しているため、クロスオーバー検出を有効にすると、必要に応じて 1 つのオーバーレイのスポークが他のオーバーレイのスポークへの直接トンネルを動的に作成できるようになります。

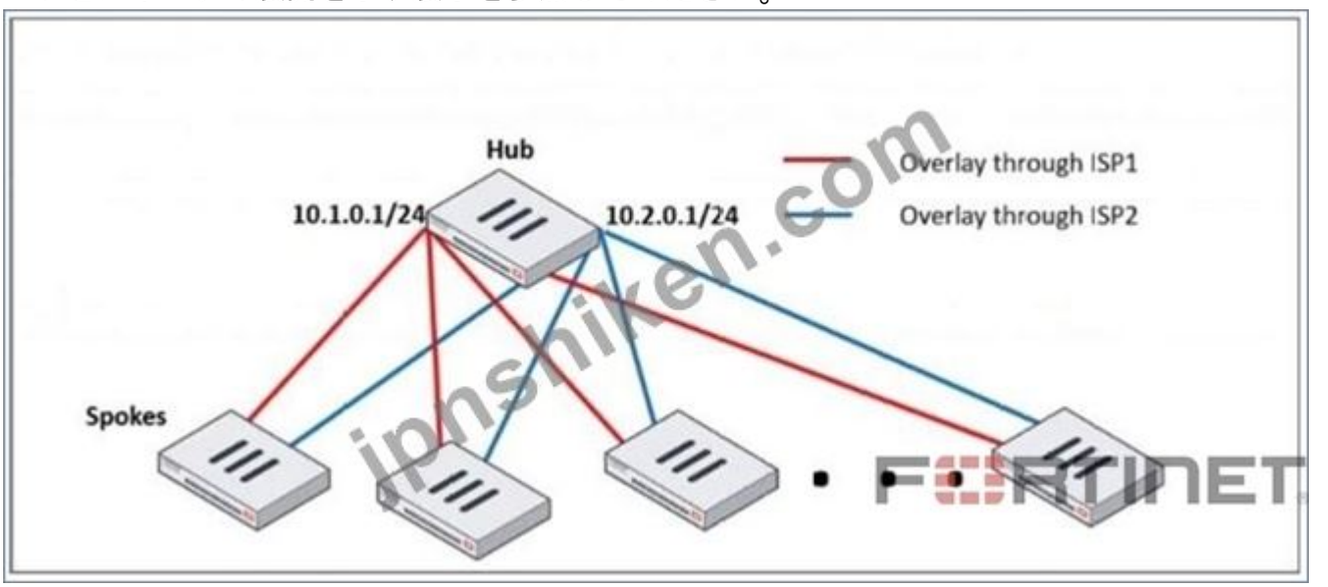
強制マルチホップを有効にする

この設定により、ループバック インターフェイスを使用する BGP ピアは、直接接続されていない場合でも接続を確立できるようになります。

ループバック アドレスを BGP ピア ソースとして使用する場合は、接続が BGP ネイバーに到達する前に複数のルーターを通過する必要がある可能性があるため、マルチホップ BGP セッションが必要です。

これは、ルートが 1 つのハブから別のハブに渡る必要がある可能性がある、複数のハブを備えた ADVPN 展開で特に役立ちます。

質問: **19**
ハブとスポークの展開を示す展示を参照してください。

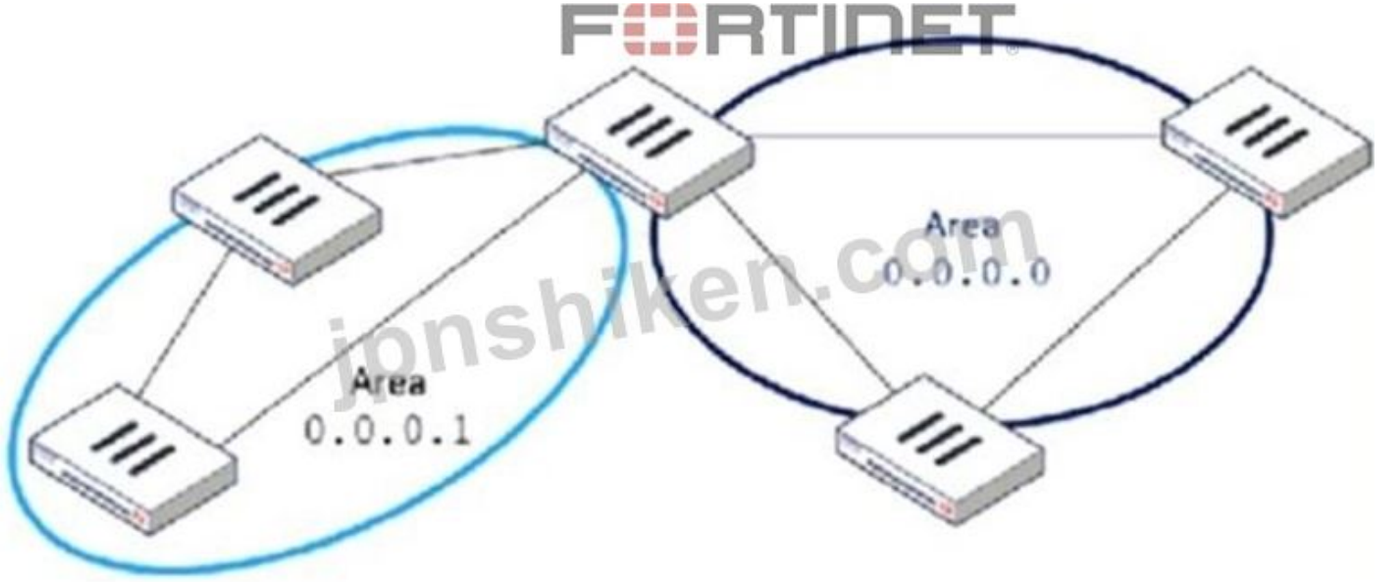


管理者は、スポークをハブに接続するための BGP 構成を含む複数のスポークを展開しています。管理者が構成を最小限に抑えることができる 2 つのコマンドはどれですか? (2 つ選択してください。)
A. 隣接グループ
B. ルートリフレクタクライアント
C. 隣接範囲
D. ibgp-enforce-multihop
正解: **(**正解を表示します**)**
隣接グループ:
このコマンドは、同じ設定を持つ複数の BGP ネイバーをグループ化し、冗長な設定を削減するために使用されます。
管理者は、スポークごとに個別の BGP 設定を定義する代わりに、ネイバー グループを作成して同じポリシーを適用することで、手作業を削減できます。
隣接範囲:
このコマンドを使用すると、ネイバー IP の範囲を動的に設定できるため、各スポーク ネイバーを手動で定義する必要性が軽減されます。
指定されたプレフィックスに一致する BGP ネイバーを自動的に追加し、導入を簡素化します。

質問: **20**
ある企業のFortiGate AとB間のIPsec VPNにおいて、VXLAN導入以降、断続的な問題が発生しています。管理者は、デフォルトのMTUである1500バイトを超えるパケットが問題の原因ではないかと考えています。
どのような状況で、インターフェースの最大 MTU 値を調整すると、IP パケットに追加のヘッダーを追加するプロトコルによって発生する問題を解決できますか?
A. FortiGate に MTU の変更を許可する FortiGuard エンタープライズ バンドルがある場合にのみ、インターフェースの MTU を調整します。

B. 最新の Fortinet SPU ファミリをサポートするすべての FortiGate デバイスのインターフェース上の MTU を調整します。
NP7、CP9、SP5。
C. パス上のすべてのデバイスが MTU インターフェースの変更を許可する制御された環境で、インターフェースの MTU を調整します。
D. PPPoE、光ファイバー、イーサネット ケーブルなどの有線接続のインターフェースのみで MTU を調整します。
正解**: (**正解を表示します**)**
IPsec VPNとVXLANを使用する場合、パケットに追加のヘッダーが追加され、デフォルトの1500バイトのMTU。これにより、断片化の問題、パケットのドロップ、パフォーマンスの低下が発生する可能性があります。
この問題を解決するには、ネットワークパス上のすべてのデバイスがMTU（最大転送単位をサポートしている場合にのみ、MTUを調整する必要があります。そうでない場合、一部のデバイスでパケットがドロップまたはフラグメント化され、問題が継続する可能性があります。
MTU を調整すると役立つ理由:
VXLAN はパケットに 50 バイトのオーバーヘッドを追加します。
IPsec は追加のカプセル化 (ESP、GRE など) を追加し、パケット サイズを増加させます。
パケットが MTU を超えると、断片化またはドロップされ、断続的な接続の問題が発生する可能性があります。
インターフェースの MTU を下げると、すべてのネットワーク デバイスでパケットがサポートされているサイズ制限内に収まるようになります。

質問**: 21**
OSPF ネットワークを示す展示を参照してください。



OSPF データベースを最適化するために管理者はどの設定を適用する必要がありますか?
A. AS 境界 FortiGate にルート マップを設定します。
B. エリア境界 FortiGate 内のエリア 0.0.0.1 をタイプ STUB に設定します。

C. AS境界FortiGateにアクセス リストを設定します。
D. エリア境界 FortiGate でエリア 0.0.0.1 をタイプ NSSA に設定します。
正解: **B (**コメントを発表する**)**
OSPFデータベースの最適化は、不要なルーティング情報を削減し、ネットワークパフォーマンスを向上させるために不可欠です。このトポロジでは、エリア0.0.0.1は、エリア境界ルータ（ABR）を介してエリア0.0.0.0（バックボーンエリア）に接続された非バックボーンエリアです。
このシナリオで OSPF を最適化するには、エリア 0.0.0.1 をスタブ エリアとして設定します。
外部ルート (OSPF 外部から) がエリア 0.0.0.1 に挿入されるのを防ぐことで、OSPF データベースのサイズを縮小します。
エリア内およびエリア間ルートのみを許可します。つまり、エリア 0.0.0.1 内のルータは外部宛先のデフォルト ルートに依存します。
交換される LSA (リンクステート アドバタイズメント) が少なくなるため、収束時間が改善され、ルーターの処理負荷が軽減されます。

質問: **22**
IT 部門は、前回のネットワーク移行中に、フェーズ 2 IPsec 構成のすべてのゼロ フェーズ セレクターがネットワーク操作に影響を与えることを発見しました。
将来の移行中にこれを防ぐための有効なアプローチを 2 つ挙げてください。(2 つ選択してください。)
A. ルーティング プロトコルを使用して、トンネル経由で許可されるサブネットを指定します。
B. IPsec 集約を構成して、各ファイアウォール ピア間の冗長性を作成します。
C. フェーズ 2 セレクターで暗号化されるセグメントを VPN に明確に示します。
D. 各ファイアウォールの IPsec インターフェイスに IP アドレスを設定して、一意のピア接続を確立し、ネットワーク操作に影響を与えないようにします。
正解: **(**正解を表示します**)**
IPsecフェーズ2のゼロフェーズセレクタとは、特定のトラフィックセレクタ（サブネット）が定義されていないことを意味し、あらゆるトラフィックがVPNトンネルを介して暗号化される可能性があります。これにより、意図しないトラフィック転送の問題が発生し、ネットワーク運用に支障をきたす可能性があります。
将来の移行中にこれが起こらないようにするには:
ルーティングプロトコルを使用することで、特定のサブネットのみがトンネル経由でアドバタイズされます。動的ルーティング（OSPFやBGPなど）は、トンネルを使用するネットワークを定義するのに役立ち、意図しないトラフィックが暗号化されるのを防ぎます。
フェーズ2セレクタを明確に定義することで、許可された送信元サブネットと宛先サブネットを明示的に指定し、すべてのトラフィックを暗号化してしまう問題を回避できます。これにより、トンネルが無関係なネットワークトラフィックに影響を与えることを防ぎます。

質問: **23**

ISDB がコンテンツ フィルタリングを適用するときに OSI モデルの第 3 層と第 4 層をブロックするのはなぜですか (2 つ選択してください)。
A. FortiGate には、FortiGuard からダウンロードされた特定のアプリケーションのすべての IP とポートの定義済みリストがあります。
B. ISDB は、FortiGuard によって事前定義されたアプリケーションの IP アドレスとポートをブロックします。
C. ISDB はプロキシ モードで動作し、OSI モデルの第 3 層および第 4 層のパケットの分析を可能にします。
D. ISDB は URL とドメインによってアクセスを制限します。
正解**: A,B (**コメントを発表する**)**
FortiGate のインターネット サービス データベース (ISDB) は、事前定義された IP アドレスとポートに基づいてアプリケーションを識別することにより、OSI モデルのレイヤー 3 (ネットワーク層) とレイヤー 4 (トランスポート層) でコンテンツ フィルタリングを実施するために使用されます。
FortiGate には、FortiGuard からダウンロードされた特定のアプリケーションのすべての IP とポートの定義済みリストがあります。
FortiGate は、FortiGuard からさまざまなインターネット サービスの IP とポートの定義済みリストを取得して更新します。
これにより、FortiGate はディープ パケット インスペクションを必要とせずに、レイヤー 3 およびレイヤー 4 で特定のサービスをブロックできるようになります。
ISDB は、FortiGuard によって事前定義されたアプリケーションの IP アドレスとポートをブロックします。
ISDB は、トラフィックを分類されたサービスの既知の IP アドレスおよびポートと照合することによって機能します。
アプリケーションまたはサービスがブロックされると、FortiGate は宛先 IP とポート番号に基づいてトラフィックを拒否し、通信を防止します。

質問**: 24**
展示品を参照してください。

OSPFコマンドの出力の一部を示しています。FortiGateのOSPFステータスを確認しているときに、図に示すような出力が表示されました。この出力に基づいて、FortiGateに関する正しい記述は2つあります。

2つの回答を選択してください）

A. FortiGate で OSPF ECMP が有効になっています。

B. FortiGate はバックアップ指定ルータです。

C. FortiGate は外部ルーティング情報を挿入します。

D. FortiGate は複数のエリアに接続されています。

正解: **A,D (**コメントを発表する**)**

包括的かつ詳細な 150 ～ 200 語の説明 (Enterprise Firewall 7.6 管理者ドキュメントの完全な抜粋より):

FortiOS 7.6 インフラストラクチャ学習ガイドと OSPF 監視に関する公式ドキュメントに基づいて、コマンド出力 get router info ospf status は OSPF プロセスに関する重要な詳細を提供します。

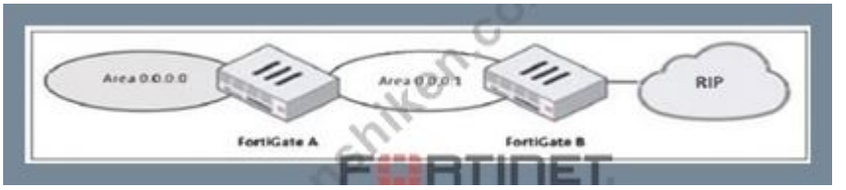
* 複数エリア（オプションD）：図の最後の行には、「このルータはABR（エリア境界ルータ）です」と明記されています。OSPFプロトコルの定義では、ABRとは複数のOSPFエリア（通常はエリア0（バックボーン）と少なくとも1つの非バックボーンエリア）に接続されたルータです。

* OSPF ECMP（オプションA）：出力はOSPFプロセスが「RFC2328に準拠している」ことを示します。RFC 2328はOSPFv2の標準規格であり、等コストマルチパス（ECMP）機能を備えています。FortiOSでは、OSPFが有効で、同じ宛先への複数の経路が同じコストを持つ場合、maximum-paths設定で特に制限されていない限り、デフォルトでECMPがサポートされます。ステータス出力にこのRFC準拠が記載されていることは、エンジンがマルチパスルーティングに対応し、サポートしていることを示しています。

オプションCは不正解です。出力ではデバイスがASBR（自律システム境界ルータ）としてラベル付けされていないため、外部ルーティング情報の挿入に必要です。オプションBは不正解です。

「ABR」はエリア階層を指し、特定のネットワークセグメントにおける選出ステータス（DR/BDR）を指していないためです。

質問: **25**
企業ネットワークの一部を示した展示を参照してください。



管理者は、エリア 0.0.0.0 で外部ネットワークを検出したいと考えています。
管理者は何を構成する必要がありますか?
A. FortiGate B で RIP 再配布を有効にします。
B. FortiGate B で distribute-route-map-in を設定します。
C. FortiGate A と B の間に仮想リンクを設定します。
D. FortiGate A および B でエリア 0.0.0.l タイプをスタブに設定します。
正解: **(**正解を表示します**)**
この図は、次のマルチエリア OSPF ネットワークを示しています。
FortiGate A は OSPF エリア 0 (バックボーン エリア) にあります。
FortiGate B は OSPF エリア 0.0.0.1 にあり、RIP ネットワークに接続されています。
OSPF エリア 0 (0.0.0.0) が外部 RIP ネットワークからルートを学習できるようにするには、FortiGate B が RIP ルートを OSPF に再配布する必要があります。
これを実現するための手順:
1. FortiGate B でルート再配布を有効にして、RIP で学習したルートを OSPF に挿入します。
2. これにより、OSPF エリア 0.0.0.1 は RIP ルートを OSPF エリア 0 (0.0.0.0) に転送できるようになり、外部ネットワークが可視化されます。