Fortinet.NSE4_FGT_AD-7.6.v2026-06-20.q64

試験コード:	NSE4_FGT_AD-7.6
試験名称:	Fortinet NSE 4 - FortiOS 7.6 Administrator
認定資格:	Fortinet
無料問題数:	64
バージョン:	v2026-06-20
アクセス数:	115
ページビュー数:	640
https://www.jpnpdf.com/Fortinet.NSE4_FGT_AD-7.6.v2026-06-20.q64-mondaishu.html	

最新問題: **1**
SSL 証明書検査が有効になっている場合、FortiGate は SSL サーバーのホスト名を識別するためにどの 3 つの情報を使用しますか? (3 つ選択してください。)
A. HTTP ヘッダーのホスト フィールド。
B. クライアント Hello メッセージ内のサーバー名表示 (SNI) 拡張。
C. サーバー証明書のサブジェクト別名 (SAN) フィールド。
D. サーバー証明書のサブジェクト フィールド。
E. サーバー証明書のシリアル番号。
Answer: B,C,D (メーッセージを残す**)**
SSL証明書検査を使用する場合、FortiGateはトラフィックを復号化しません。SSLハンドシェイクの開始時にHelloメッセージを交換する際に、FortiGateはClient HelloからTLSプロトコルの拡張であるサーバ名表示 $SNI）を解析します。SNIはFortiGateにSSLサーバのホスト名を伝え、サーバ証明書を受信する前にDNS名と照合して検証します。SNIが交換されない場合、FortiGateはサーバ証明書のSubjectフィールドまたはSAN $ubject Alternative Name）フィールドの値に基づいてサーバを識別します。

最新問題: **2**
管理者は、一部のユーザーが SSL VPN 接続を確立できない一方で、他のユーザーは問題なく接続できることに気付きました。
管理者はまず何を確認すべきでしょうか?
A. 影響を受けるユーザーが正しいポート番号を使用していることを確認します。
B. ユーザー トラフィックがファイアウォール ポリシーに該当することを確認します。
C. 強制トンネリングが有効になっていて、すべてのトラフィックがSSL VPN経由で再ルーティングされていることを確認します。
D. SSL VPNトンネルインターフェースでHTTPSサービスが有効になっていることを確認します。
Answer: (解答を表示する**)**
ユーザー トラフィックが SSL VPN を許可する適切なファイアウォール ポリシーと一致しない場合、ユーザーは接続を確立できないため、これが最初に確認する必要がある点になります。

最新問題: **3**
SSL 証明書検査が有効になっている場合、FortiGate は SSL サーバーのホスト名を識別するためにどの 3 つの情報を使用しますか? (3 つ選択してください。)
A. HTTP ヘッダーのホスト フィールド。
B. クライアント Hello メッセージ内のサーバー名表示 (SNI) 拡張。

C. サーバー証明書のサブジェクト別名 (SAN) フィールド。
D. サーバー証明書のサブジェクト フィールド。
E. サーバー証明書のシリアル番号。
Answer: B,C,D (メーッセージを残す**)**
FortiGate デバイスで SSL 証明書検査が有効になっている場合、システムは次の 3 つの情報を使用して SSL サーバーのホスト名を識別します。
クライアントHelloメッセージのServer Name Indication（SNI）拡張B） SNIは、SSL/TLSプロトコルのクライアントHelloメッセージの拡張です。クライアントが接続しようとしているホスト名を示します。これにより、FortiGateはSSLハンドシェイク中にサーバーのホスト名を識別できます。
サーバー証明書のサブジェクト代替名（SAN）フィールド（C）サーバー証明書のSANフィールドには、証明書が有効な追加のホスト名またはIPアドレスが記載されています。FortiGateはこのフィールドを検査してサーバーのIDを確認します。
サーバー証明書のサブジェクトフィールド（D）サブジェクトフィールドには、証明書が発行されたプライマリホスト名またはドメイン名が含まれます。FortiGateは、SSL証明書検査中にこの情報を使用してサーバーのIDを照合および検証します。

最新問題**: 4**
図を参照してください。NOCチームは、NOC_Access管理者プロファイルを使用してFortiGate GUIに接続します。非アクティブな状態でGUIセッションが早期に切断されないように要求しています。NOCチームからのこの特定の要求に応えるために、管理者はどのような設定を行う必要がありますか？

A. すべてのプロファイル設定が有効になるように、NOC_Access をリストの先頭に移動します。
B. NOC_Access 管理プロファイルの Override Idle Timeout パラメータのオフライン値を増やします。
C. アクセスを保証するために、すべての NOC_Access ユーザーに super_admin ロールが割り当てられていることを確認します。
D. config system accprofile NOC_Access の admintimeout 値を増やします。
Answer: D (メーッセージを残す**)**
管理者アクセスプロファイルの admintimeout 設定は、GUI セッションの非アクティブタイムアウトを制御します。この値を大きくすると、自動切断までのセッション継続時間が長くなります。

最新問題**: 5**
アクティブ認証を有効にするファイアウォール ポリシーを示す図を参照してください。

アクティブな認証方法を使用して外部 Web サイトにアクセスしようとすると、ユーザーにログイン プロンプトが表示されません。

この状況の最も可能性の高い理由は何でしょうか?
A. ファイアウォール ポリシーではサービス DNS が必要です。
B. FSSO 構成でリモート ユーザー グループを正しく設定する必要があります。
C. このユーザーに一致するユーザー アカウントが存在しません。
D. リモート ユーザー グループは宛先に追加されません。
Answer: A (メッセージを残す**)**
DNSは通常、HTTPによって使用され、ユーザーがウェブサイトでIPアドレスではなくドメイン名を使用できるようにします。DNSは基本プロトコルであり、適切な認証プロトコルトラフィックを最初に確認する必要がある可能性が高いため、許可されます。ただし、DNSサービスが通過するには、ポリシーで許可されているように定義されている必要があります。

最新問題**: 6**
SD-WAN パフォーマンス SLA に関する次の 3 つの記述のうち正しいものはどれですか。(3 つ選択してください。)
A. セッション損失とジッターに依存します。
B. FortiGate デバイスの状態を監視します。
C. すべての SLA ターゲットを設定できます。
D. これらは、SD-WAN ルールの最低コスト戦略に適用されます。
E. 能動的または受動的に測定できます。
Answer: C,D,E (メッセージを残す**)**
FortiOS 7.6では、SD-WANパフォーマンスSLAを使用してリンク品質を測定し、SD-WANルールの決定に影響を与えます。以下の3つの記述は正しいです。
C. すべてのSLAターゲットを設定できます。
真実
SD-WAN パフォーマンス SLA により、管理者は次の設定を行うことができます。
レイテンシー
ジッター
パケット損失
平均オピニオンスコア（MOS）（音声）
これらのメトリックのしきい値は、SLA ごとに完全に構成可能です。
これは、SD-WAN パフォーマンス SLA 構成セクションに明示的に記載されています。
D . これらは、SD-WAN ルールの最低コスト戦略に適用されます。
真実
パフォーマンス SLA は、通常、最低コスト (SLA ベース) 戦略で使用されます。
この戦略では :
FortiGate は、SLA 要件を満たす最も低コストのリンクを選択します。
リンクが SLA に違反している場合は、選択から除外されます。
E . 能動的または受動的に測定できます。
真実
FortiOS は以下をサポートします:
アクティブプローブ（ping/HTTPなどの合成プローブ）
パッシブ測定（実際のトラフィック統計に基づく）
管理者は、展開と要件に応じて SLA の測定方法を選択できます。
他の選択肢が間違っている理由

A . セッション損失とジッターに依存しています。
正しくない
SLA は、パケット損失、遅延、ジッターを測定します。
セッション損失は、FortiOS の SLA メトリックではありません。
B. FortiGateデバイスの状態を監視します。
正しくない
パフォーマンス SLA は、FortiGate システムの健全性やデバイスの状態ではなく、リンクの品質を監視します。

最新問題**: 7**
HA クラスターについて正しい記述はどれですか? (2 つ選択してください。)
A. HA クラスターは、インバンド管理インターフェイスとアウトオブバンド管理インターフェイスの両方を同時に持つことはできません。
B. 管理者がプライマリ デバイスでインターフェイスをダウンに設定すると、リンク フェールオーバーによってフェールオーバーがトリガーされます。
C. ハートビート インターフェイスをスニッフィングする場合、管理者は IP アドレス 169.254.0.2 を確認する必要があります。
D. HA 増分同期には、FIB エントリと IPsec SA が含まれます。
Answer: B,D (メーッセージを残す**)**
プライマリ デバイスでインターフェイスをダウンに設定すると、リンク フェールオーバー検出によりフェールオーバーがトリガーされます。
HA 増分同期には、セッションの継続性を維持するための転送情報ベース (FIB) エントリと IPsec セキュリティ アソシエーション (SA) が含まれます。

最新問題**: 8**
展示品を参照してください。

FortiGateはファイアウォール認証に設定されています。外部ウェブサイトにアクセスしようとしても、ログインプロンプトが表示されません。
この状況の最も可能性の高い理由は何でしょうか?
A. ファイアウォール ポリシーではサービス DNS が必要です。
B. ユーザーが間違ったユーザー名を使用しています。
C. このユーザーに一致するユーザー アカウントが存在しません。
D. リモート ユーザー グループは宛先に追加されません。
Answer: A (メーッセージを残す**)**
ユーザーがまだ認証されていない場合は、DNS トラフィックを許可できます。
認証に使用されるアプリケーション層プロトコル (HTTP/HTTPS/FTP/Telnet) では、ホスト名の解決がしばしば必要になります。
DNS サービスは、ポリシー内のサービスとして明示的にリストされている必要があります。

最新問題**: 9**

図を参照してください。NOCチームは、NOC_Access管理者プロファイルを使用してFortiGate GUIに接続します。非アクティブな状態でGUIセッションが早期に切断されないように要求しています。NOCチームからのこの特定の要求に応えるために、管理者はどのような設定を行う必要がありますか？

A. すべてのプロファイル設定が有効になるように、NOC_Access をリストの先頭に移動します。
B. NOC_Access 管理プロファイルの Override Idle Timeout パラメータのオフライン値を増やします。
C. アクセスを保証するために、すべての NOC_Access ユーザーに super_admin ロールが割り当てられていることを確認します。
D. config system accprofile NOC_Access の admintimeout 値を増やします。
Answer: B (メーッセージを残す**)**
「アイドル タイムアウトの上書き」設定を使用して、管理者プロファイルごとにアイドル タイムアウト設定を上書きできます。
管理者プロファイルを設定することで、非アクティブタイムアウトを延長し、集中監視用のGUIを容易に利用できるようになります。また、 Override Idel Timeout」設定により、config system accprofile の admintimeout 値をアクセスプロファイルごとに上書きできます。

最新問題: 10
添付資料を参照してください。FTP用の新しいウイルス対策プロファイルを作成するときに、ウイルス対策スキャンスイッチがグレー表示になっているのはなぜですか？

A. このプロファイルでは、検査されたプロトコルのいずれもアクティブではありません。
B. RAM が 2 GB 未満の FortiGate は、ウイルス対策スキャン機能をサポートしていません。

C. システム -> 機能の可視性でウイルス対策スキャンが無効になっています。
D. プロファイルの機能セットはフローベースですが、プロキシベースである必要があります。
Answer: A (メッセージを残す**)**
検査対象として 1 つ以上のプロトコルを有効にし、指定したアクションで選択したプロトコルのウイルス対策スキャンを有効にします。
https://docs.fortinet.com/document/fortigate/7.6.4/administration-guide/922096/inspection-mode- 機能比較

最新問題**: 11**
本社のFortiGateには、アグレッシブモードで構成された複数のダイヤルアップIPsec VPNがあります。ダイヤルアップユーザーをそれぞれの部門のVPNトンネルに接続する必要があります。
ユーザーをトンネルに一致させるために構成できるフェーズ 1 のどの設定ですか?
A. ローカルゲートウェイ
B. デッドピア検出
C. ピアID
D. IKE モード設定
Answer: C (メッセージを残す**)**
FortiOS 7.6 では、同じ FortiGate 上に複数のダイヤルアップ IPsec VPN が設定されている場合 (特にアグレッシブ モードの場合)、FortiGate は接続クライアントがどのフェーズ 1 設定と一致する必要があるかを識別する必要があります。
FortiGateがダイヤルアップIPsecトンネルを選択する方法
ダイヤルアップ VPN の場合:
リモートピア（ユーザーまたはデバイス）に固定IPアドレスがありません
HQ FortiGateには複数のフェーズ1インターフェースが存在する可能性がある
FortiGate は、IKE フェーズ 1 中に送信された識別情報を使用して、正しいトンネルを選択します。アグレッシブ モードの動作アグレッシブ モードでは、フェーズ 1 中に ID 情報がクリア テキストで送信されます。これにより、FortiGate は、着信ピアを正しいフェーズ 1 構成と一致させることができます。ピア ID が正しい答えである理由 C)。ピア ID ピア ID (IKE ID とも呼ばれる) は次の目的で使用されます。
リモートピアを識別する
複数のダイヤルアップトンネルを区別する
一般的なピア ID 形式:
完全修飾ドメイン名
ユーザーFQDN
キーID
FortiGateは受信したピアIDをフェーズ1の構成と照合して正しいトンネルを選択します。これは、次の場合に文書化され推奨される方法です。
ユーザーを異なる部門のトンネルにマッピングする
アグレッシブモードで複数のダイヤルアップIPsec VPNをサポート
他の選択肢が間違っている理由
A). ローカルゲートウェイリモート ユーザーではなく、ローカル FortiGate インターフェース/IP を識別します。
B). デッドピア検出トンネルの選択ではなく、トンネルの健全性の監視にのみ使用されます。
D). IKE モード構成フェーズ 1 トンネルの選択ではなく、IP アドレスの割り当てと設定のプッシュに使用されます。

最新問題**: 12**
新しい管理者は、DC エージェント モードを使用して FortiGate で FSSO 認証を構成しています。
予想されるプロセスの一部ではないステップはどれですか?
A. DC エージェントはログイン イベント データを FortiGate に直接送信します。

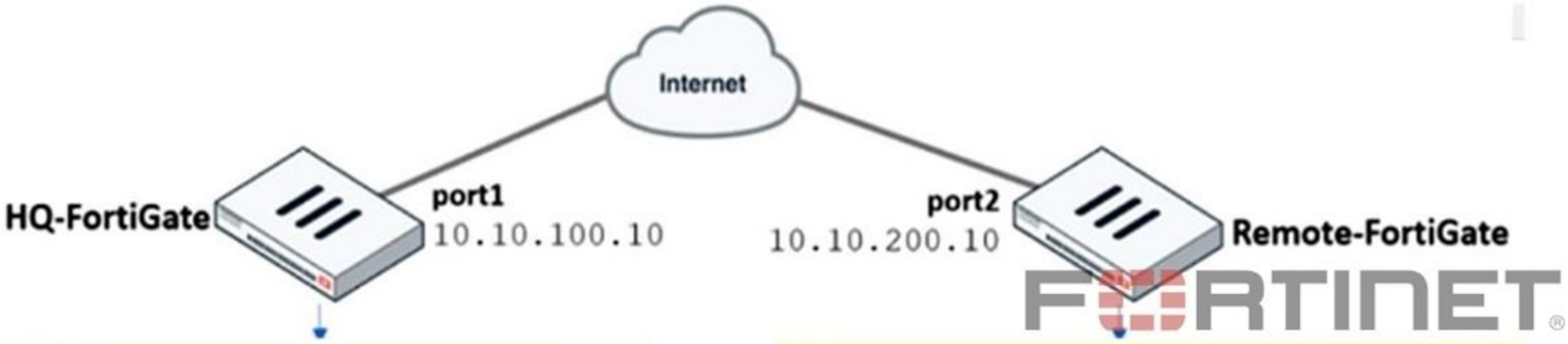
B. ユーザーは Windows ドメインにログインします。
C. コレクター エージェントはログイン イベント データを FortiGate に転送します。
D. FortiGate は、FSSO リスト内の IP アドレスに基づいてユーザー ID を決定します。
Answer: (解答を表示する**)**
DCエージェントモードでは、ドメインコントローラにインストールされたDCエージェントがログオンイベント（例イベントID 4624）をリアルタイムでキャプチャします。そして、この情報をコレクタエージェントにプッシュします。専用マシン上でサービスとして実行されるコレクタエージェントは、この情報を統合し、FortiGateファイアウォールに転送する役割を担います。FortiGateはこのデータを受信し、ユーザーのIPアドレスに基づいて適切なセキュリティポリシーを適用します。

最新問題**: 13**
FortiGate が SSL/SSH 完全検査を実行するときに、無効な証明書を検出した場合の対応方法を決定できます。
無効な証明書を検出したときに FortiGate が実行できる有効なアクションはどれですか (3 つ選択してください)。
A. 許可する
B. 信頼して許可
C. 許可と警告
D. ブロック
E. ブロックと警告
Answer: (解答を表示する**)**
FortiGate が SSL/SSH 完全検査を実行する場合、無効な証明書を検出したときに次のいずれかのアクションを実行するように設定できます。
許可 → トラフィックを制限なく通過させます。
許可と警告 → トラフィックを許可しますが、証明書の問題についてユーザーに警告します。
ブロック → 安全でない接続を防ぐためにトラフィックを完全に拒否します。

最新問題**: 14**
FortiGate ファイアウォール ポリシーはアクティブ認証で構成されていますが、ユーザーは Web サイトにアクセスするときに認証できません。
ユーザーが認証できない場合でも、FortiGate はどのプロトコルを許可する必要がありますか?
A. LDAP
B. TACASC+
C. ケルベロス
D. DNS
Answer: D (メーッセージを残す**)**
アクティブ認証 (HTTP/HTTPS/FTP/Telnet など) および DNS で使用される認証ダイアログを表示するには、ファイアウォール ポリシーでプロトコルを許可する必要があります。

最新問題**: 15**
展示品を参照してください。

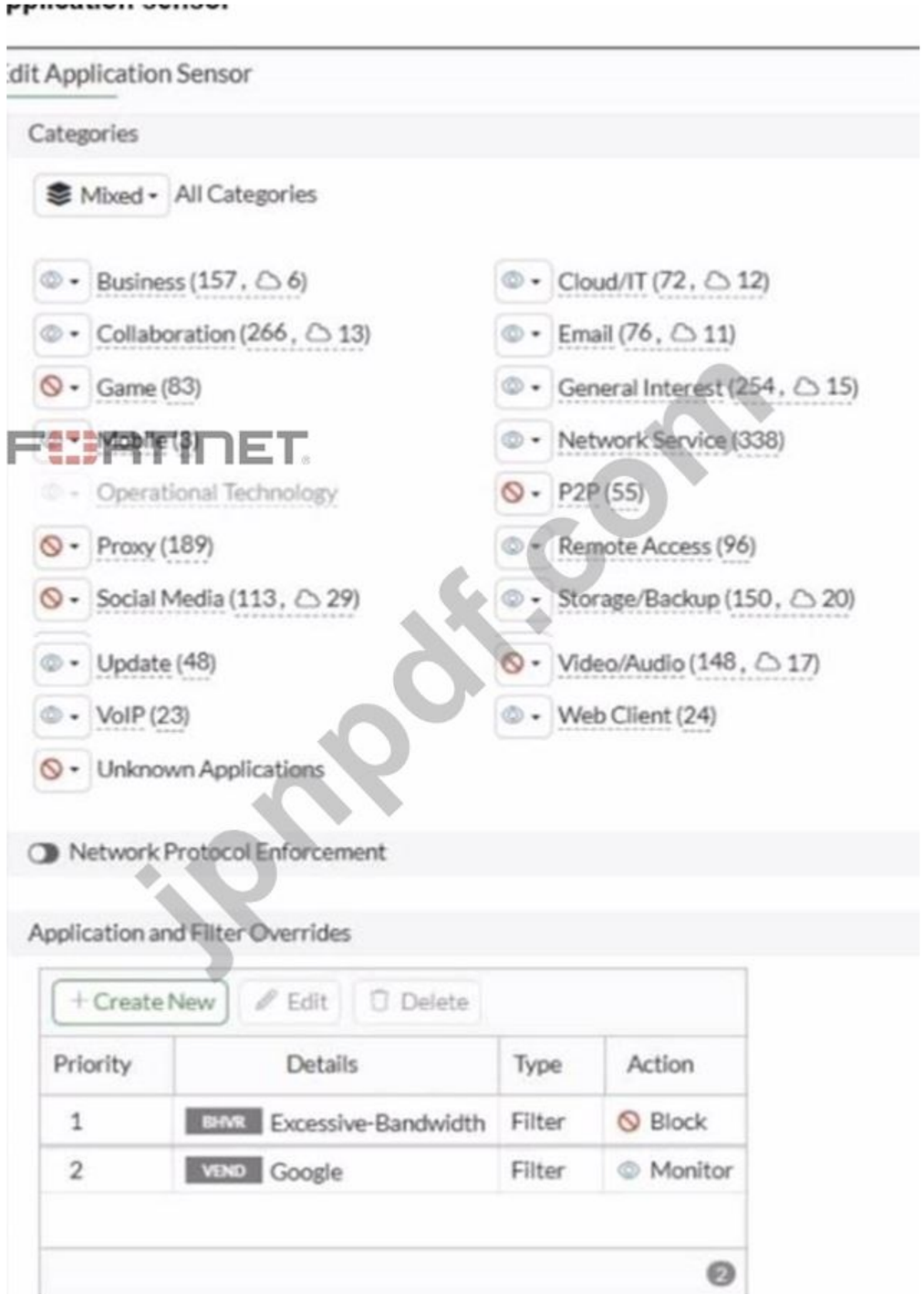
IPsec tunnel configuration



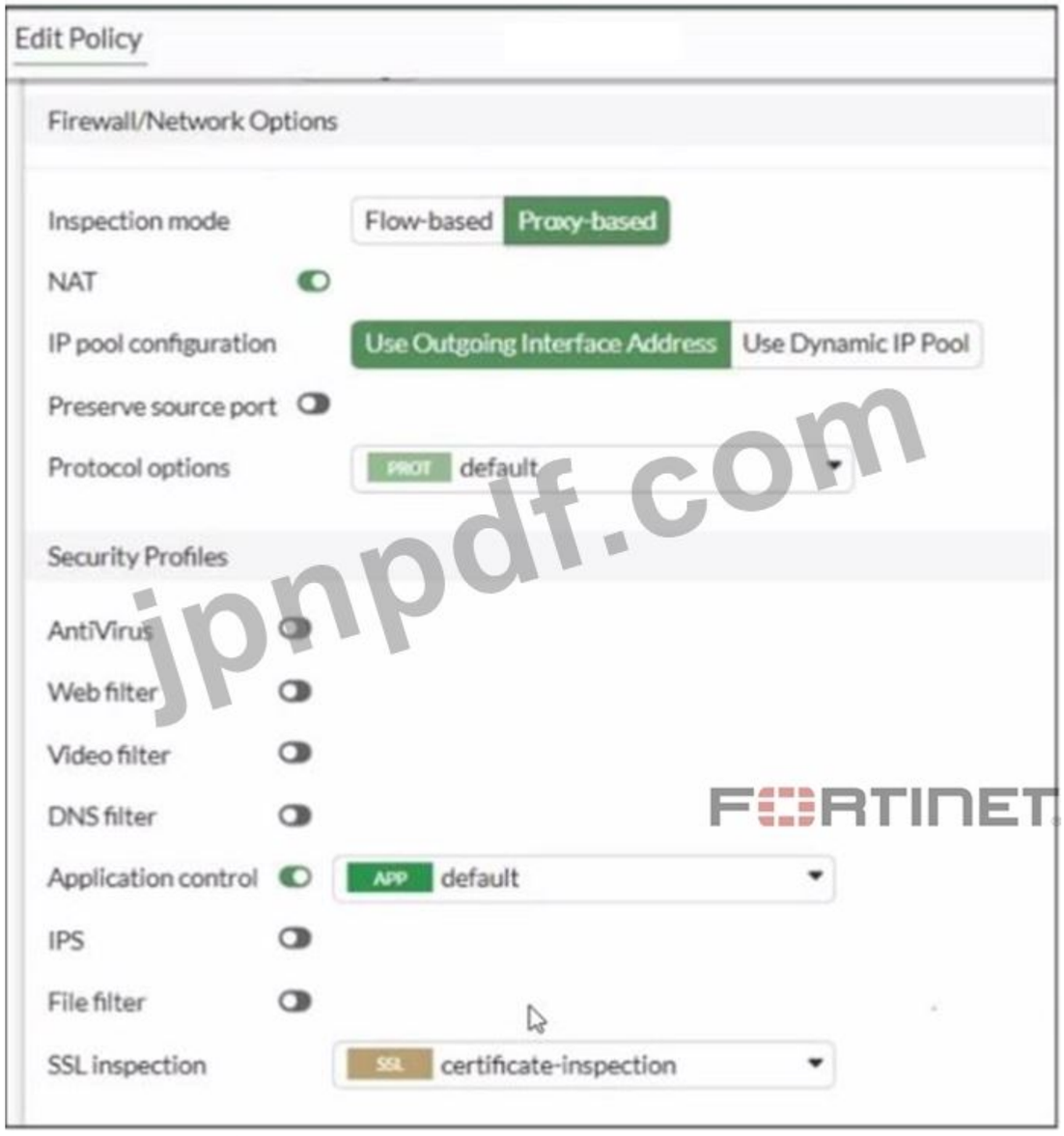
ネットワーク管理者は、2台のFortiGateデバイス間のIPsecトンネルのトラブルシューティングを行っています。管理者は、フェーズ1が起動に失敗したことを確認しました。また、両方のFortiGateデバイスで事前共有鍵を再入力し、一致していることを確認しました。
フェーズ 1 の構成と図に基づいて、管理者はフェーズ 1 を起動するためにどの 2 つの構成変更を行うことができますか? (2 つ選択してください。)
A. HQ-FortiGate で、IKE モードをメイン (ID 保護) に設定します。
B. リモート FortiGate で、ポート 2 をインターフェースとして設定します。
C. HQ-FortiGate で、Diffie-Helman グループ 2 を無効にします。
D. 両方の FortiGate デバイスで、Dead Peer Detection をオンデマンドに設定します。
Answer: A,B (メーッセージを残す**)**
HQ-FortiGateではIKEフェーズ1モードがアグレッシブに設定されていますが、リモートFortiGateではメイン（ID保護）に設定されています。フェーズ1が起動するには、両側で同じIKEモードを使用する必要があります。そのため、HQ-FortiGateをメインモードに変更することで、この不一致を解消できます。
リモートFortiGateでは、フェーズ1インターフェースはポート1に設定されていますが、図によると、IPアドレス10.10.200.10を持つWAN側インターフェースはポート2です。IPsec設定のローカルインターフェースは物理WANインターフェースと一致する必要があるため、トンネルを確立するにはポート2に変更する必要があります。

最新問題**: 16**
FortiGate HA 構成の同期に関して正しい記述はどれですか (2 つ選択してください)。
A. デバイスのチェックサムが相互に比較され、構成が同じであることを確認します。
B. 増分構成同期は、プライマリ FortiGate デバイスで行われた変更からのみ実行されます。
C. HA クラスタ内の任意の FortiGate デバイスで行われた変更から、増分構成同期が発生する可能性があります。
D. 一部の構成項目が他の HA メンバーに同期されていないため、デバイスのチェックサムは互いに異なります。
Answer: A,C (メーッセージを残す**)**
新しいFortiGateをクラスタに追加すると、プライマリFortiGateは自身の設定チェックサムを新しいセカンダリFortiGateの設定チェックサムと比較します。チェックサムが一致しない場合、プライマリFortiGateは自身の設定全体をセカンダリFortiGateにアップロードします。
初期同期が完了した後、HA クラスタ デバイス (プライマリまたはセカンダリ) の構成に変更が加えられるたびに、増分同期によって、同じ構成変更が HA ハートビート リンクを介して他のすべてのクラスタ デバイスに送信されます。

最新問題**: 17**
展示物を参照してください。



Firewall policy



図に示すように、アプリケーション センサーと対応するファイアウォール ポリシーを実装しました。
Google アプリケーションにはアクセスできませんが、www.fortinet.com にはアクセスできます。
この問題を解決するには、どの 2 つのアクションを実行しますか? (2 つ選択してください)

A. SSL 検査をディープコンテンツ検査に設定します。
B. アプリケーションとフィルタのオーバーライドセクションでGoogleを上に移動して、優先順位を設定します。
C. セキュリティ プロファイルの URL カテゴリに「Google.com」を追加します。
D. 検査モードをフローベースに変更します
E. アプリケーションとフィルタのオーバーライドセクションでGoogleのアクション を許可に設定します

Answer: (解答を表示する**)**
展示品より:
ファイアウォール ポリシーではアプリケーション制御が有効になっており、SSL 検査に証明書検査が使用されます。
アプリケーション センサーには、次の順序 (優先順位) のアプリケーション オーバーライドとフィルター オーバーライドがあります。
過剰な帯域幅とアクションブロック
Google（ベンダーフィルター）アクションモニター
FortiOSでは、アプリケーションとフィルタのオーバーライドは優先度（トップダウン）に基づいて評価されます。最初に一致したオーバーライドが適用されます。トラフィックが以前のオーバーライドでブロックに一致した場合、後続のオーバーライドで監視/許可に一致してもブロックされます。
www.fortinet.com は機能しているのに、Google アプリが機能しない理由:
多くの Google アプリケーションは、特定のサービスとトラフィック パターンに応じて、過剰な帯域幅の動作/シグネチャとして検出される (またはトリガーされる) 可能性があります。
過剰帯域幅（ブロック）が Google（監視）の上にあるため、Google 関連のトラフィックが最初のルールに一致し、Google のオーバーライドが評価される前にブロックされる可能性があります。
www.fortinet.com へのアクセスは、そのトラフィックが過剰な帯域幅のオーバーライドと一致しないため機能します。
したがって、解決するには:
B). 「アプリケーションとフィルタのオーバーライド」セクションで Google を上に移動して、優先度を高く設定します。これにより、より広範なブロックのオーバーライドが適用される前に、Google が Google のオーバーライドと一致するようになります。
E) 「アプリケーションとフィルターの上書き」セクションで Google のアクションを 「許可」に設定します。これにより、優先度の高い一致が発生した場合に Google アプリケーションが明示的に許可されます (トラブルシューティングとアクセスの確保のために 「監視」よりも強力です)。
他のオプションがここで最適ではない理由:
「ディープコンテンツ検査」は、より多くの HTTPS アプリケーションを識別するのに役立ちますが、この図にはすでに特定の Google オーバーライドが設定されていることが示されています。当面の問題は、オーバーライドの評価順序とアクションです。
CはWebフィルタのURLカテゴリに関連していますが、問題はアプリケーション制御の動作で発生しています。
/vendor がオーバーライドします。
D (フローベース) は、オーバーライドの優先順位とアクションの競合を修正するために必要ではありません。

最新問題**: 18**
NGFW プロファイルベース モードの 2 つの機能は何ですか? (2 つ選択してください。)
A. NGFW プロファイルベース モードでは、中央ソース NAT ポリシーの使用が必要になります。
B. NGFW プロファイル ベース モードは、個々の VDOM ではなく、グローバルにのみ適用できます。
C. NGFW プロファイルベース モード ポリシーは、フロー検査とプロキシ検査の両方をサポートします。
D. NGFW プロファイル ベース モードでは、ファイアウォール ポリシーでアプリケーションと Web フィルタリング プロファイルを適用することをサポートします。
Answer: (解答を表示する**)**
FortiGateのNGFW（次世代ファイアウォール）プロファイルベースモードでは、ポリシーでフローベースとプロキシベースの両方のインスペクションモードを使用できるため、セキュリティとパフォーマンスの要件に応じた柔軟性が得られます。さらに、プロファイルベースモードでは、ファイアウォールポリシーにアプリケーションとWebフィルタリングのプロファイルを直接適用できるため、トラフィックをきめ細かく制御できます。

最新問題**: 19**
添付資料を参照してください。添付資料は、FortiGateデバイスにおけるシステムパフォーマンス出力と、高メモリ使用量しきい値のデフォルト設定を示しています。

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

システムパフォーマンス出力に基づいて、どのような 2 つの結果が考えられますか? (2 つ選択してください。)

A. FortiGate は節約モードに入りました。

B. 管理者はコンソール ポート経由でのみ FortiGate にアクセスできます。

C. 管理者は設定を変更できます。

D. FortiGate は新しいセッションをドロップします。

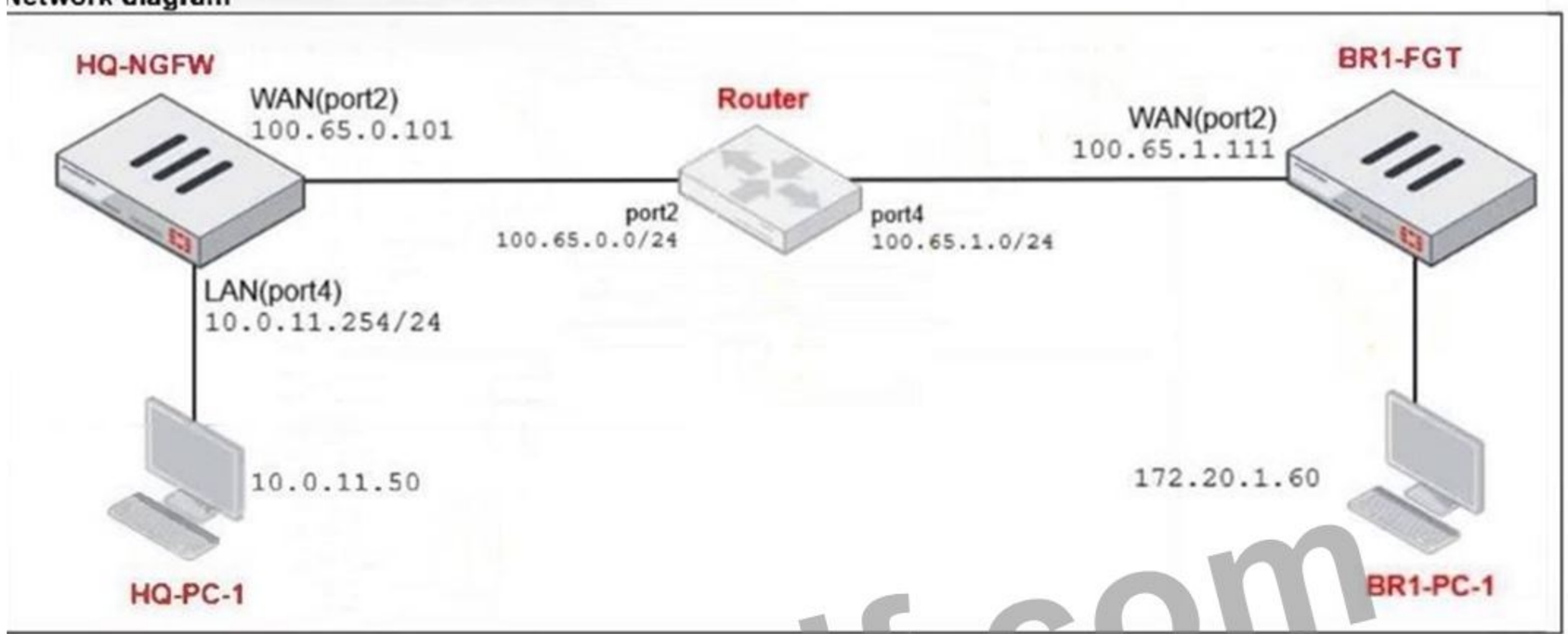
Answer: A,D (メーッセージを残す**)**

FGはデフォルトで88%で節約モードに入り、この時点では設定の変更はできません。また、追加の設定がない場合、FGは検査が必要なセッションを破棄します。95%になると、すべての新規セッションが破棄されます。

最新問題**: 20**

添付資料を参照してください。添付資料には、ネットワークに接続されたFortiGateデバイスの図、IPプール設定、ファイアウォールポリシーオブジェクトが示されています。

Network diagram



NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

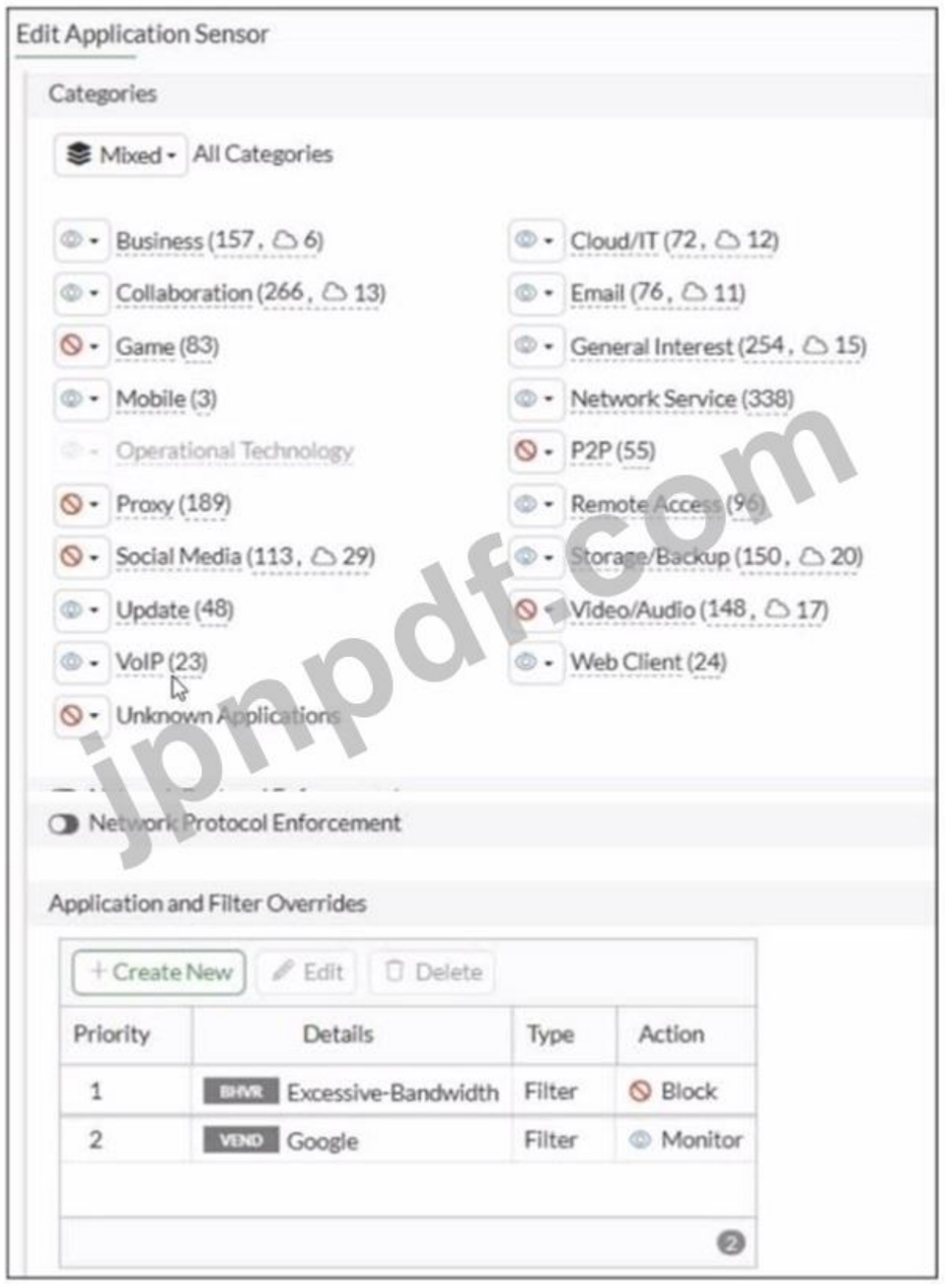
Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

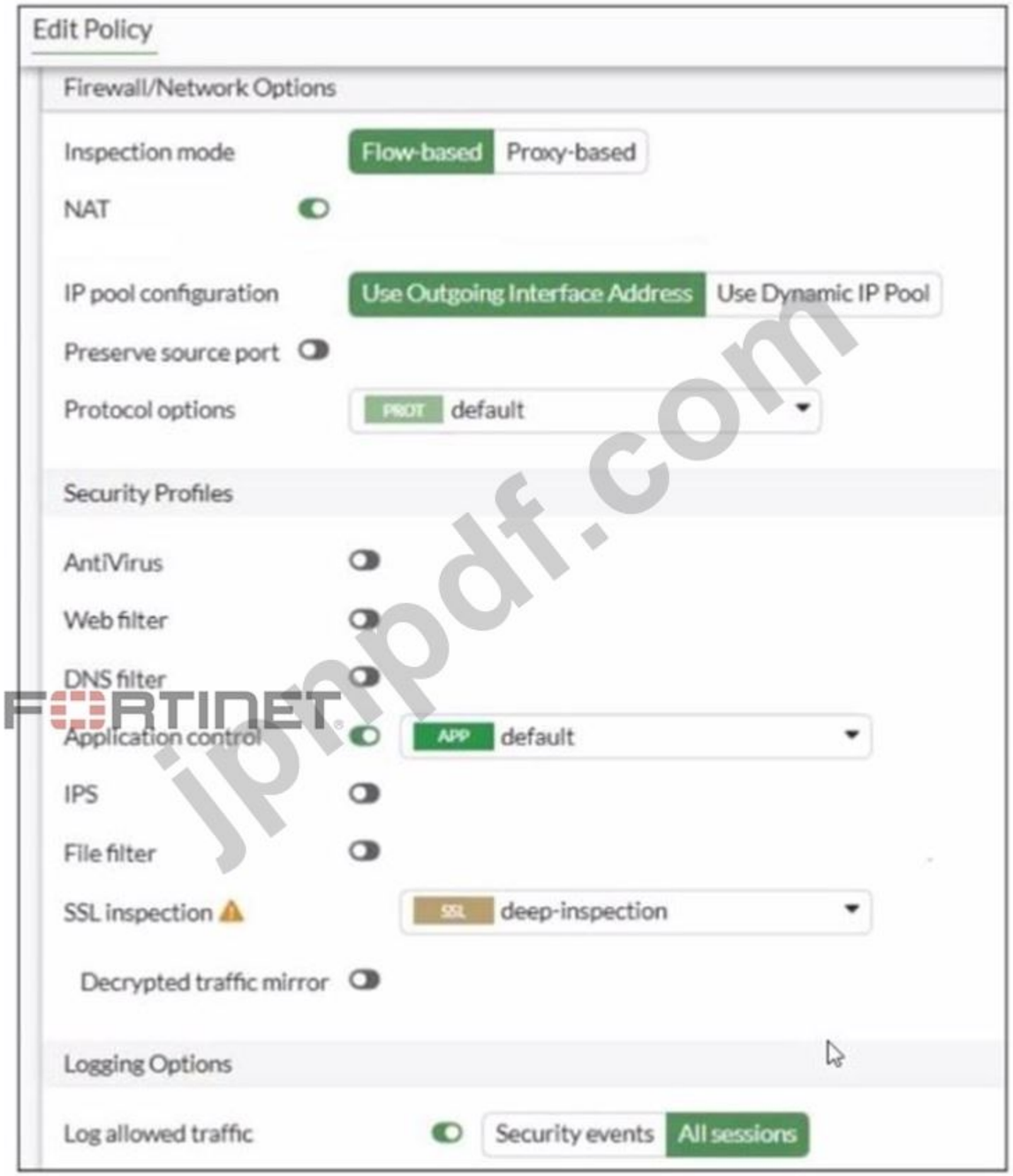
WAN（port2）インターフェースのIPアドレスは100.65.0.101/24です。LAN（port4）インターフェースのIPアドレスは10.0.11.254/24です。HQ-PC-1（10.0.11.50）のユーザーがBR-FGT（100.65.1.111）のIPアドレスにpingを実行した場合、どのIPアドレスがトラフィックのソースNAT（SNAT）に使用されますか？
A. 100.65.0.101
B. 100.65.0.49
C. 100.65.0.99
D. 100.65.0.149
Answer: C (メーッセージを残す**)**
pingトラフィックポリシーは、外部IP範囲を持つSNAT-Remote1というIPプールを使用します。
100.65.0.99。したがって、このポリシーに一致するトラフィック（HQ-PC-1からBR1-FGTへのping）は、
ソース NAT の場合は 100.65.0.99。

最新問題**: 21**
展示物を参照してください。

Application sensor



Firewall policy



図に示すように、アプリケーション センサーと対応するファイアウォール ポリシーを実装しました。
これらの構成から観察できる 2 つの要素は何ですか? (2 つ選択してください。)
A. 過剰な帯域幅のアプリケーションとフィルターのオーバーライド設定に基づいて YouTube アクセスがブロックされます。

B. カテゴリ フィルター設定に基づいて Facebook へのアクセスがブロックされます。
C. Facebook へのアクセスは許可されていますが、ビデオ/オーディオ カテゴリ フィルターの設定に基づいて Facebook ビデオを再生することはできません。
D. Google アプリケーションとフィルターのオーバーライド設定に基づいて YouTube 検索が許可されます。
Answer: (解答を表示する**)**
展示品より:
アプリケーション制御センサーには次の主要な設定があります。
アプリケーションとフィルターのオーバーライド
優先度1: 過剰帯域幅 (タイプ: フィルター)アクションブロック
優先度2: Google (タイプ: フィルター)とアクションモニター
表示されるカテゴリ アクションには、ブロックに設定されたソーシャル メディア (このカテゴリには Facebook が含まれます) が含まれます。
ファイアウォール ポリシーでは以下を使用しています:
フローベース検査
アプリケーション制御が有効 (プロファイル: デフォルト)
ディープ インスペクションが有効 (HTTPS 内のアプリケーションの識別に役立ちます)
ログ記録が有効
FortiOS は、次のようにアプリケーション制御を適用します (アプリケーション制御プロファイル内でトップダウン)。
オーバーライドは優先度によって評価されます (優先度が最も高いものが最初)。
最初に一致したオーバーライドによって、そのトラフィックのアクション (ブロック/監視/許可) が決定されます。
カテゴリベースのアクションは、オーバーライドが最初に一致しない限り、それらのカテゴリに該当するアプリケーションに適用されます。
Aが正しい理由
A . YouTube へのアクセスは、過剰な帯域幅のアプリケーションとフィルターのオーバーライド設定に基づいてブロックされます。
プロファイルは、最高のオーバーライド優先度で過剰帯域幅動作フィルターを明示的にブロックします。
YouTube トラフィックが過剰帯域幅の動作に一致すると検出された場合、FortiGate はオーバーライドによりブロック アクションを適用します。
これは優先度のオーバーライドであるため、優先度の低いエントリよりも前に適用されます。
Bが正しい理由
B. カテゴリフィルター設定に基づいて Facebook へのアクセスがブロックされます。
アプリケーション センサーには、ブロック アクションが構成されたソーシャル メディアが表示されます。
Facebook はソーシャル メディアに分類されるため、アプリケーション制御に一致するとブロックされます。
Cが正しくない理由
C. Facebook へのアクセスは許可されていますが、Facebook ビデオを再生することはできません...
ソーシャル メディア カテゴリがブロックに設定されているため、Facebook はカテゴリ レベルでブロックされます (ビデオの再生だけでなく)。
Dが正しくない理由
D . YouTube 検索は Google のオーバーライドに基づいて許可されます...
Google のオーバーライド アクションは、許可ではなく監視です。
「モニター」はトラフィックをログに記録/検出しますが、ブロック条件を上書きしてトラフィックを「許可」することはありません。
また、YouTube トラフィックが「Google」として許可される方法で処理される保証はなく、一致するブロック条件 (Excessive-Bandwidth など) が依然として優先されます。

最新問題**: 22**
FortiGate で以下のコマンドを設定しました。

この構成は FortiGate にどのような影響を与えますか?

A. FortiGate はすべてのインターフェースで厳密な RPF を有効にし、非対称ルーティングではポートが有効になります。

B. FortiGate はすべてのインターフェースで厳密な RPF を有効にし、ポートは RPF チェックから除外されます。

C. グローバル設定が優先され、FortiGate はすべてのインターフェースで厳密な RPF を有効にします。

D. ポート1はフレキシブルRPFが有効になり、他のすべてのインターフェースはストリクトRPFが有効になります。

Answer: (解答を表示する**)**

最新問題**: 23**

管理者はFortiGate上でadd-routeを有効にしたダイヤルアップIPsec VPNを設定しました。しかし、ルーティングテーブルにスタティックルートが表示されません。このシナリオについて正しい記述はどれですか？ 2つ選択してください。）

A. add-route が適切に機能するには、管理者は静的ルートではなくポリシー ルートを使用する必要があります。

B. 管理者はフェーズ2が正常に確立されていることを確認する必要があります

C. 管理者は、フェーズ 2 セレクターでリモート ネットワークを正しく定義する必要があります。

D. 管理者はダイヤルアップ インターフェイスで動的ルーティング プロトコルを有効にする必要があります。

Answer: B,C (メーッセージを残す**)**

FortiGateでダイヤルアップIPsec VPNを使用する場合、add-routeが有効になっていると、FortiGateはトンネルから十分なネゴシエート情報を取得できた場合にのみ、対応するルートをインストールします。FortiOS 7.6では、これはルートがフェーズ2（クイックモード）セレクターに関連付けられ、IPsec SAが実際にアップ状態になったときに動的に作成されることを意味します。

B . 管理者はフェーズ2が正常に確立されていることを確認する必要があります

これは必須です。FortiGateは、フェーズ1が存在する、または設定が存在するという理由だけで、add-routeルートをインストールするわけではありません。ルートはトンネルが実際に使用可能になったときに追加されますが、そのためにはフェーズ2（IPsec SA）が確立されている必要があります。フェーズ2が確立されていない場合、アクティブなSAは存在せず、FortiGateは関連ルートをルーティングテーブルに挿入しません。

したがって、静的ルートが表示されない場合は、フェーズ 2 が起動していないというのが正しい説明の 1 つです。

C . 管理者はフェーズ2セレクタでリモートネットワークを正しく定義する必要があります。これも必須です。ダイヤルアップトンネルの場合、FortiGateはフェーズ2セレクタ（プロキシID）で定義されたリモートサブネットから追加するルートを導出します。フェーズ2のリモートネットワークが欠落している、間違っている、またはネゴシエーションが不可能なほど広すぎる／狭すぎる場合、トンネルは確立されない（つまりルートがない）か、インストールされるルートが管理者の期待と一致しなくなります。

したがって、もう 1 つの正しい説明は、フェーズ 2 のリモート ネットワークが正しく定義されていないため、正しいルートが作成されないということです。

他の選択肢が間違っている理由

A. 静的ルートの代わりにポリシールート

ルート追加機能はポリシールートを必要としません。これは具体的には、IPsecトンネル/SAおよびフェーズ2セレクタネットワークに関連付けられたルート（ルートテーブルエントリ）を挿入する機能です。

D). 動的ルーティングプロトコルを有効にする

動的ルーティングプロトコル（OSPF/BGP/RIP）は、add-route には必要ありません。add-route は動的ルーティングとは独立しており、ネゴシエートされたセレクタに基づいてローカルにルートを設定することで機能します。

最新問題**: 24**

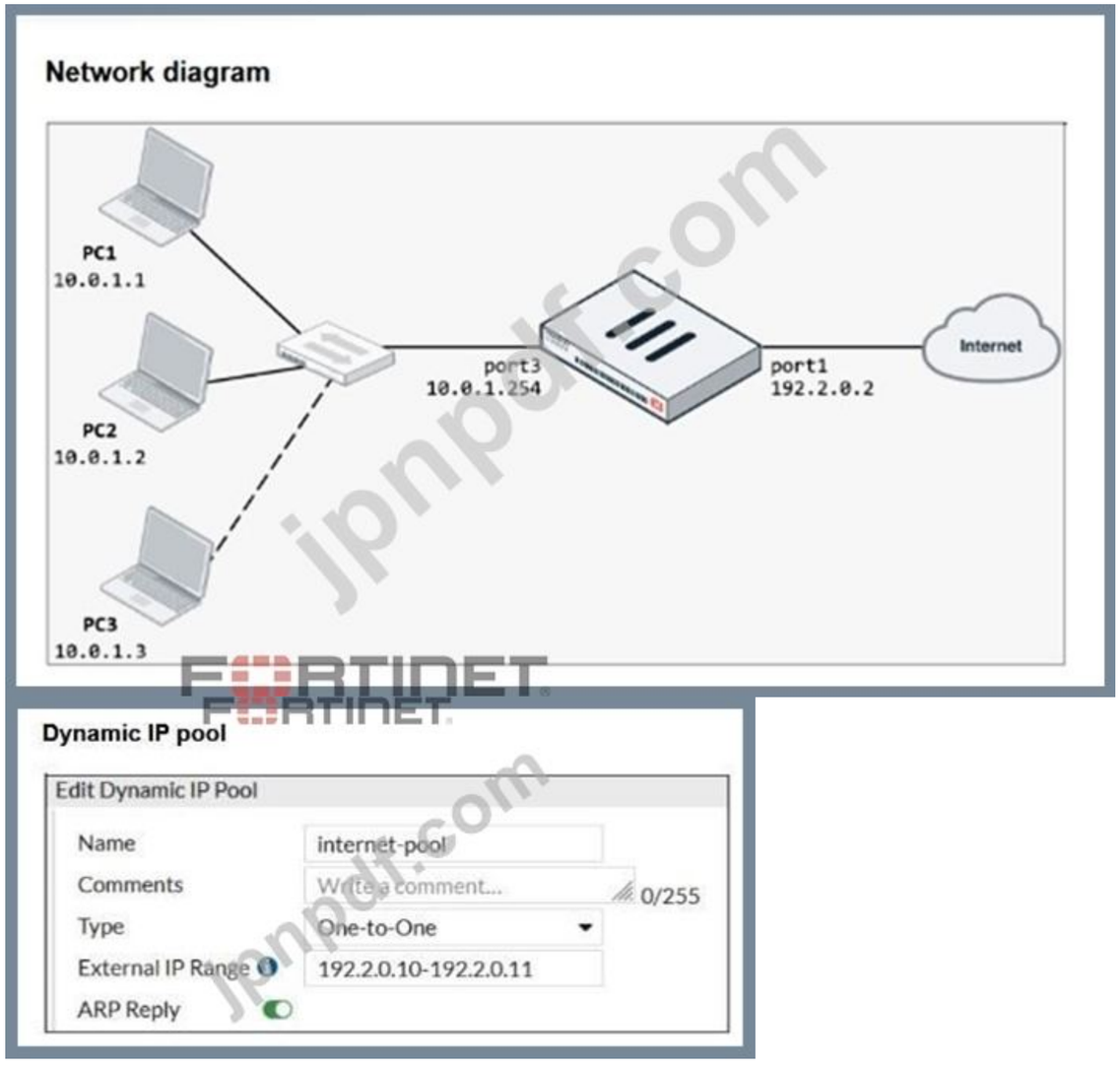
FortiGate でサポートされている IPsec IKEv1 認証の機能はどれですか (2 つ選択してください)。
A. 交換されるパケット数が少なくなり、認証が高速化する拡張認証（XAuth）
B. 認証方法としての事前共有鍵と証明書署名
C. 認証方法として証明書署名を設定する場合、リモートピアに証明書は必要ありません。
D. リモートピアにユーザー名とパスワードの提供を要求する拡張認証（XAuth）
Answer: (解答を表示する**)**
認証に関しては、どちらのバージョンもPSKと証明書署名をサポートしています。IKEv1のみがXAuthをサポートしていますが、IKEv2はXAuthと同等のEAPをサポートしています。

最新問題**: 25**
FortiGate は FortiAnalyzer および FortiManager と統合されています。
ファイアウォール ポリシーを作成するときに、機能を強化し、FortiAnalyzer および FortiManager でのログ記録を有効にするために、管理者はどの属性を含める必要がありますか?
A. ポリシーID
B. ログID
C. ユニバーサルユニーク識別子
D. シーケンスID
Answer: (解答を表示する**)**
ファイアウォール オブジェクトまたはポリシーを作成するときに、UUID 属性が追加され、ログにこれらの UUID を記録して、FortiManager または FortiAnalyzer との統合時に機能を向上させることができます。

最新問題**: 26**
管理者は、一部のユーザーが SSL VPN 接続を確立できない一方で、他のユーザーは問題なく接続できることに気付きました。
管理者はまず何を確認すべきでしょうか?
A. 影響を受けるユーザーが正しいポート番号を使用していることを確認します。
B. ユーザー トラフィックがファイアウォール ポリシーに該当することを確認します。
C. 強制トンネリングが有効になっていて、すべてのトラフィックがSSL VPN経由で再ルーティングされていることを確認します。
D. SSL VPNトンネルインターフェースでHTTPSサービスが有効になっていることを確認します。
Answer: A (メーッセージを残す**)**
質問の重要な部分は、一部のユーザーは接続でき、一部のユーザーは接続できないという点です。これは、ファイアウォール ポリシーの問題ではなく、クライアント側の接続の問題であることを強く示唆しています (ポリシーはトンネルが確立された後にのみ適用されます)。
SSL-VPN の場合、ユーザーが接続に失敗したときに最初に確認する必要があるのは、正しい接続設定 (特にポート) を使用しているかどうかです。

最新問題**: 27**
ファイアウォール ポリシーを構成する場合、ポリシー ID に関して正しいのは次のどれですか。
A. GUI または CLI に関係なく、ファイアウォール ポリシーを作成するときにポリシー ID を指定することが必須です。
B. ファイアウォール ポリシー ID は、ファイアウォール ポリシー内のポリシー実行順序を識別します。
C. CLI でポリシー ID 0 のポリシーを作成できます。
D. ポリシーを作成した後は、ポリシー ID を編集することはできません。
Answer: (解答を表示する**)**
ファイアウォール ポリシーが作成されると、そのポリシー ID は固定され、変更できなくなります。この ID は、FortiGate 構成内でポリシーを一意に識別します。

最新問題: **28**
展示物を参照してください。



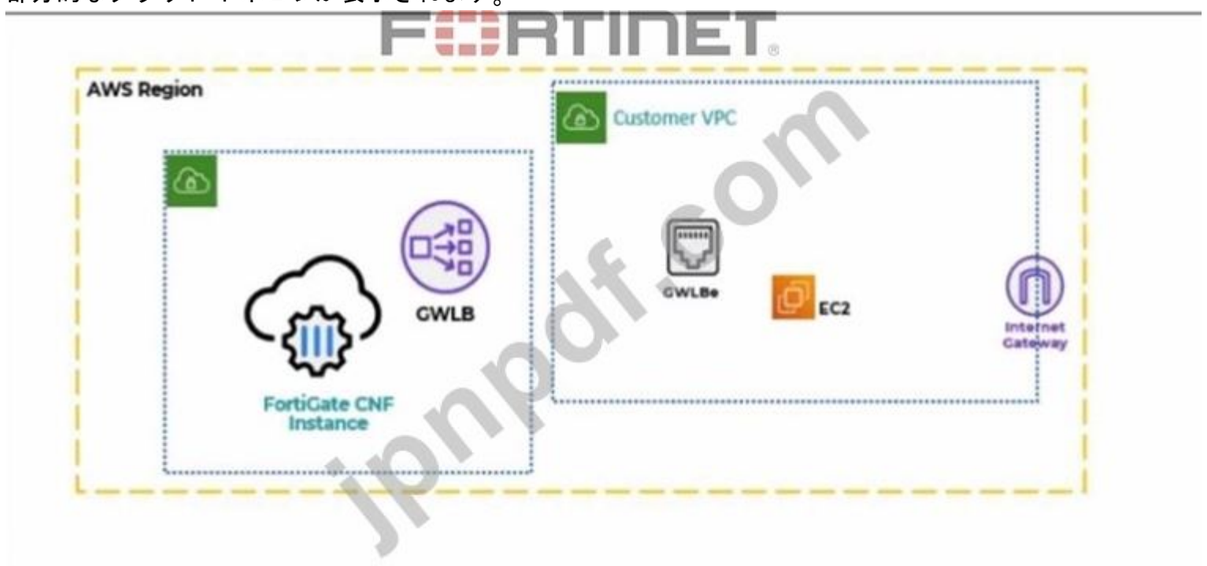
Firewall policy

図には、ネットワークに接続された FortiGate デバイスの図と、FortiGate デバイス上のファイアウォール ポリシーと IP プール構成が示されています。
PC1とPC2の2台のPCはFortiGateの背後に接続されており、インターネットに正常にアクセスできます。しかし、管理者が3台目のPC（PC3）をネットワークに追加すると、そのPCはインターネットに接続できなくなります。
展示に示されている情報に基づいて、管理者が PC3 の接続の問題を解決するために使用できる 2 つの構成オプションはどれですか? (2 つ選択してください。)
A. IP プール構成で、タイプをオーバーロードに設定します。
B. ファイアウォール ポリシー構成で、ソース フィールドにアドレス オブジェクトとして 10.0.1.3 を追加します。
C. PC3 のアドレスのみを送信元として一致する別のファイアウォール ポリシーを設定し、そのポリシーをリストの先頭に配置します。
D. IP プール構成で、endip を 192.2.0.12 に設定します。
Answer: (解答を表示する)
IPプールタイプを「1対1」に設定すると、プール内のパブリックIP（192.2.0.10～192.2.0.11）と同じ数の内部ホストのみがNATを使用できます。タイプを「オーバーロード」に変更すると、すべての内部ホスト（PC3を含む）が利用可能なパブリックIPを共有できるようになり、PC3はインターネットにアクセスできるようになります。
あるいは、1 対 1 を維持しながらプールを 192.2.0.10 ～ 192.2.0.12 に拡張すると、別のパブリック IP が追加され、3 番目の内部ホスト (PC3) をマップしてインターネットにアクセスできるようになります。

最新問題**: 29**
HA オーバーライド設定が有効になっている場合のプライマリ FortiGate 選択プロセスは何ですか?
A. 接続された監視対象ポート > 優先度 > HA稼働時間 > FortiGateのシリアル番号
B. 接続されている監視対象ポート > 優先度 > システム稼働時間 > FortiGateのシリアル番号
C. 接続された監視対象ポート > HA稼働時間 > 優先度 > FortiGateのシリアル番号
D. 接続された監視対象ポート > システム稼働時間 > 優先度 > FortiGateのシリアル番号
Answer: (解答を表示する)
HA オーバーライドが有効になっている場合、FortiGate は次の選択順序を使用します: 接続されている監視対象ポートの数、デバイスの優先度、HA の稼働時間、最後に FortiGate のシリアル番号 (タイブレー

カーとして)。

最新問題: **30**
展示品を参照してください。
部分的なクラウド トポロジが表示されます。



AWS に FortiGate クラウドネイティブ ファイアウォール (CNF) をデプロイしました。
展開中に、EC2 インスタンスからのトラフィックを処理するために FortiGate CNF が作成する必要があるコンポーネントはどれですか?
A. 顧客のVPCとGWLBe
B. 顧客の仮想プライベートクラウド (VPC) 内のゲートウェイロードバランサエンドポイント (GWLBe)
C. CNF VPC、顧客VPC、およびGWLB
D. 顧客VPC内のGWLB、GWLBe、およびインターネットゲートウェイ (IGW)
Answer: B (メーッセージを残す**)**
AWS 向け FortiGate クラウドネイティブ ファイアウォール (CNF) アーキテクチャでは、顧客 VPC 内のワークロード (EC2 インスタンスなど) からのトラフィックは、AWS ゲートウェイ ロードバランサ (GWLB) テクノロジーを使用してセキュリティ サービス (FortiGate CNF) にリダイレクトされます。
ワークロードトラフィックを GWLB に誘導するために、顧客の VPC 内に存在する必要がある主要な AWS コンポーネントは次のとおりです。
ゲートウェイ ロード バランサ エンドポイント (GWLBe)
このエンドポイントは、顧客の VPC ルートが指すもの (たとえば、デフォルト ルートまたはサブネット ルート エントリ) であり、EC2 トラフィックに対する FortiGate CNF 検査パスの透過的な挿入を可能にします。
他のオプションが正しくない理由:
A: CNF は 「顧客 VPC を作成」しません (つまり、顧客が所有します)。ここで作成される関連する項目は 「GWLBe」のみであり、VPC 全体ではありません。
C: 顧客 VPC は CNF によって作成されず、GWLB は通常 CNF サービス側の一部です。質問では具体的に、EC2 インスタンスからのトラフィックを処理するために何を作成する必要があるのかを尋ねています (顧客 VPC に GWLBe が必要です)。
D: CNF は顧客の VPC にインターネット ゲートウェイ (IGW) を作成しません。また、IGW はトラフィックを FortiGate CNF に誘導するために必要な CNF 作成コンポーネントではありません。

最新問題: **31**

本社のFortiGateには、アグレッシブモードで構成された複数のダイヤルアップIPsec VPNがあります。ダイヤルアップユーザーをそれぞれの部門のVPNトンネルに接続する必要があります。
ユーザーをトンネルに一致させるために構成できるフェーズ 1 のどの設定ですか?
A. ローカルゲートウェイ
B. デッドピア検出
C. ピアID
D. IKE モード設定
Answer: C (メーッセージを残す**)**
FortiOS 7.6 では、同じ FortiGate 上に複数のダイヤルアップ IPsec VPN が設定されている場合 (特にアグレッシブ モードの場合)、FortiGate は接続クライアントがどのフェーズ 1 設定と一致する必要があるかを識別する必要があります。
FortiGateがダイヤルアップIPsecトンネルを選択する方法
ダイヤルアップ VPN の場合:
リモートピア（ユーザーまたはデバイス）に固定IPアドレスがありません
HQ FortiGateには複数のフェーズ1インターフェースが存在する可能性がある
FortiGate は、IKE フェーズ 1 中に送信された識別情報を使用して、正しいトンネルを選択します。アグレッシブ モードの動作アグレッシブ モードでは、フェーズ 1 中に ID 情報がクリア テキストで送信されます。これにより、FortiGate は、着信ピアを正しいフェーズ 1 構成と一致させることができます。ピア ID が正解である理由 C . ピア ID ピア ID (IKE ID とも呼ばれる) は次の目的で使用されます。
リモートピアを識別する
複数のダイヤルアップトンネルを区別する
一般的なピア ID 形式:
完全修飾ドメイン名
ユーザーFQDN
キーID
FortiGateは受信したピアIDをフェーズ1の構成と照合して正しいトンネルを選択します。これは、次の場合に文書化され推奨される方法です。
ユーザーを異なる部門のトンネルにマッピングする
アグレッシブモードで複数のダイヤルアップIPsec VPNをサポート
他の選択肢が間違っている理由
A. ローカルゲートウェイ
リモート ユーザーではなく、ローカル FortiGate インターフェイス/IP を識別します。
B . デッドピア検出
トンネルの選択ではなく、トンネルの健全性の監視にのみ使用されます。
D . IKEモード設定
フェーズ 1 トンネルの選択ではなく、IP アドレスの割り当てと設定のプッシュに使用されます。

最新問題: 32
SSL VPN ユーザーが VPN から切断した後も、認証されたセッションがアクティブなままにならないようにする必要があります。
どのような構成でこれを実現できるでしょうか?
A. ファイアウォール認証セッション タイムアウトを SSL VPN セッション タイムアウトよりも短く設定します。

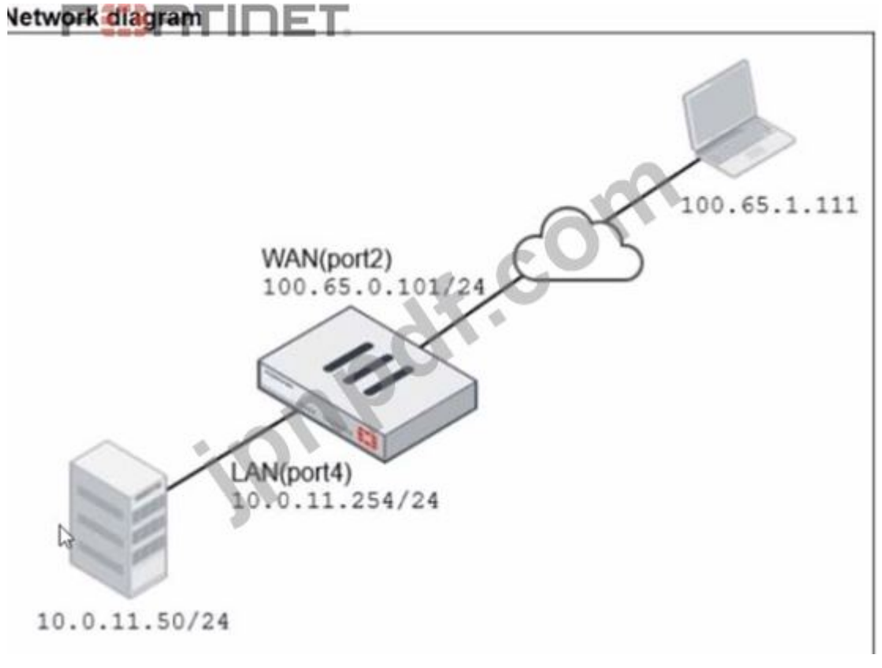
B. ユーザーが切断した後、アクティブなファイアウォール認証セッションを手動でクリアします。
C. SSL VPN アイドル タイムアウトを増やして、早期切断の可能性を減らします。
D. SSL VPNセッションが終了したときにファイアウォール認証セッションを強制的に終了する設定を有効にします
Answer: D (メーッセージを残す)
認証済みのSSL VPNユーザーセッションが切断後も継続しないようにするには、SSL VPNセッションの終了時にファイアウォール認証セッションを強制的に終了する設定を有効にする必要があります。これにより、VPNが切断されると、関連するファイアウォール認証状態が直ちにクリアされ、意図しないアクセスを防止できます。

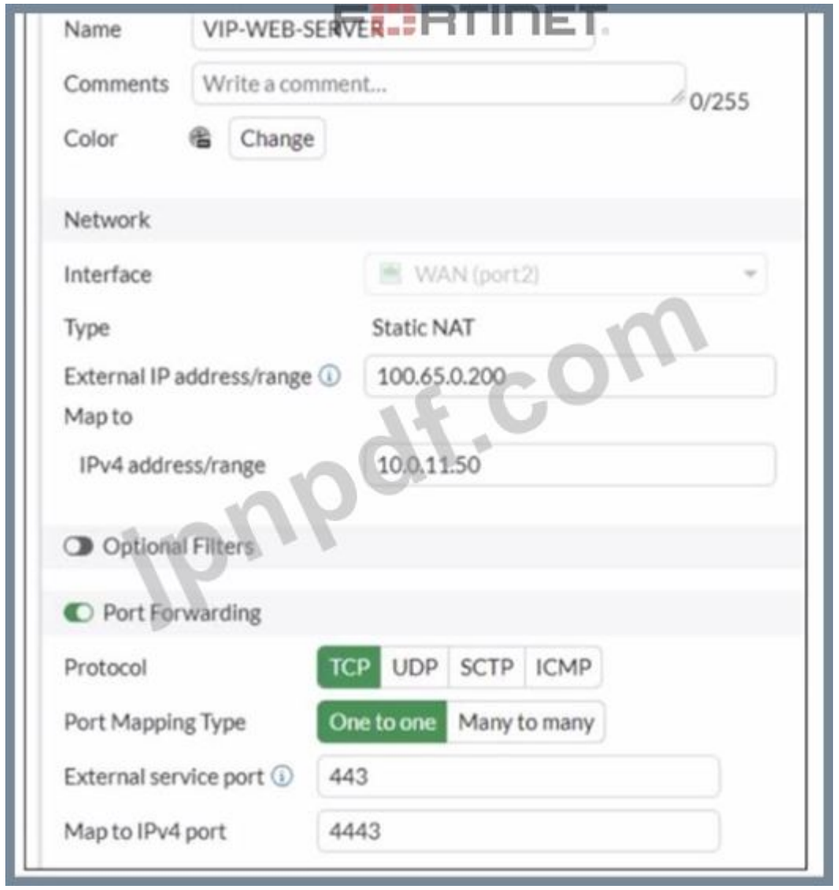
最新問題: **33**
展示品を参照してください。
RADIUS サーバーの構成が表示されます。

管理者が新しい RADIUS サーバーの構成を追加しました。構成中に、管理者はすべてのユーザー グループに含めるを有効にしました。RADIUS 構成ですべてのユーザー グループに含めるを有効にすると、どのような影響がありますか?
A. このオプションは、RADIUS サーバーと、そのサーバーに対して認証できるすべてのユーザーを、すべての FortiGate ユーザー グループに配置します。
B. このオプションは、認証に必要なすべての FortiGate ユーザーとグループを RADIUS サーバー (この場合は FortiAuthenticator) に配置します。
C. このオプションは、RADIUS サーバーと、そのサーバーに対して認証できるすべてのユーザーをすべての RADIUS グループに配置します。
D. このオプションは、FortiGate 上の LDAP サーバーに使用されるグループを含む、すべてのユーザーをすべての RADIUS ユーザー グループに配置します。
Answer: A (メーッセージを残す)
FortiOS 7.6 の認証とユーザー グループのドキュメントに基づくと、正解は A です。
「すべてのユーザーグループに含める」の意味（FortiOS 7.6）
FortiGate で RADIUS サーバーを構成するときに、すべてのユーザー グループに含めるを有効にすると、非常に具体的かつ文書化された効果が得られます。
設定された RADIUS サーバー オブジェクトは、すべての FortiGate ユーザー グループに自動的に追加されます。
その結果、追加のグループ フィルタリング (RADIUS 属性など) が適用されない限り、その RADIUS サーバーに対して正常に認証されたユーザーは、すべての FortiGate ユーザー グループの有効なメンバーになります。
これにより、異なるユーザー グループを参照する複数のファイアウォール ポリシー全体で同じ外部認証ソースを受け入れる必要がある場合に構成が簡素化されます。

この動作については、FortiOS 7.6 管理者ガイドの RADIUS 認証サーバーおよびユーザー グループ」に明確に説明されています。
オプションAが正しい理由
FortiGate ユーザー グループには次のものが含まれます。
ローカルユーザー
LDAPサーバー
RADIUSサーバー
すべてのユーザー グループに含めるを有効にすると、FortiGate は次のようになります。
RADIUS サーバーを既存および将来のすべての FortiGate ユーザー グループに挿入します。したがって、この RADIUS サーバー経由で認証するすべてのユーザーは、すべての FortiGate ユーザー グループで暗黙的に許可されます。
これはまさにオプション A で説明されている内容です。
他の選択肢が間違っている理由
B: FortiGateはユーザーやグループをRADIUSサーバーにプッシュしません。認証は常にFortiGateからRADIUSサーバーに向けて開始されます。
C: FortiGate は RADIUS 側のグループ定義を管理または変更しません。
D: LDAP および RADIUS ユーザー グループは別々の認証メカニズムです。この設定は LDAP グループを結合したり、影響を与えたりしません。

最新問題**: 34**
展示物を参照してください。





Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	✓ ACCEPT		NAT
☐	Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	✓ ACCEPT		Disabled

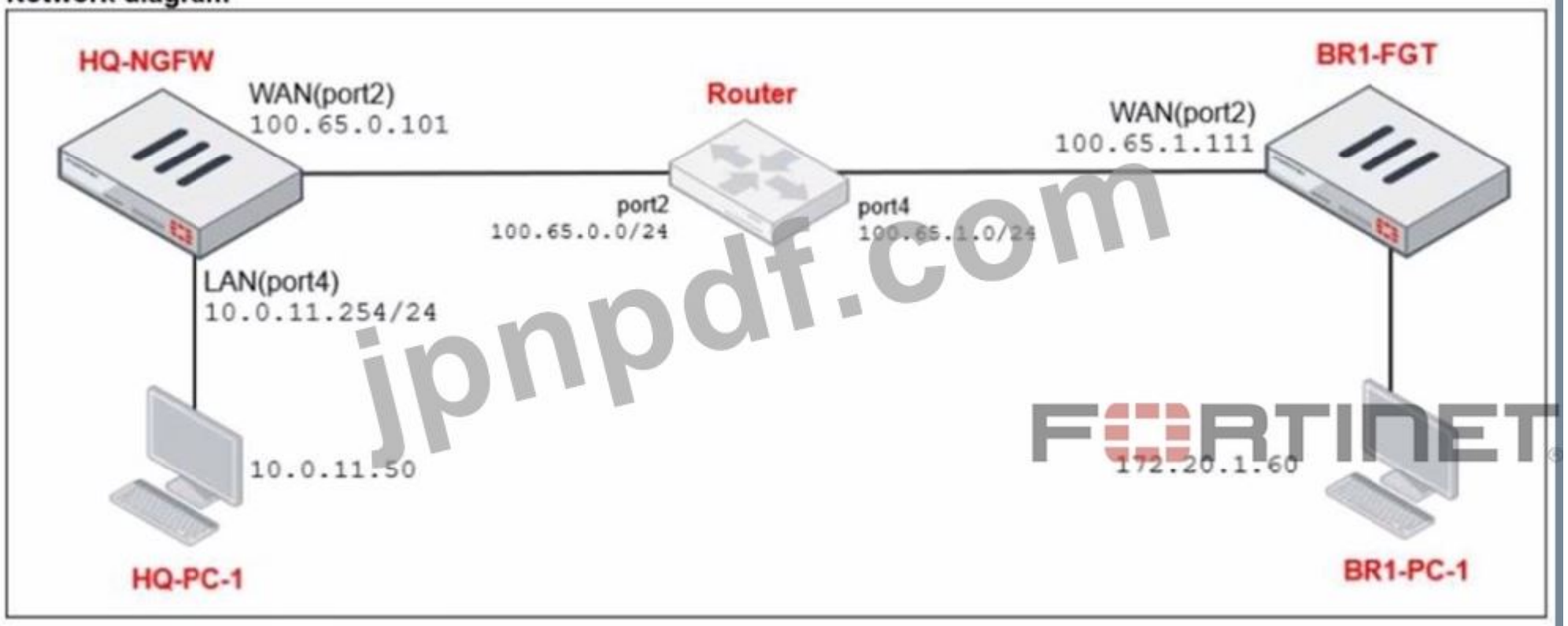
ネットワーク VIP オブジェクトに接続された FortiGate デバイスとファイアウォール ポリシー構成の図が表示されます。
WAN（ポート2）インターフェースにはIPアドレスがあります
100.65.0.101/24。
LAN（ポート4）インターフェースにはIPアドレスがあります
10.0.11.254/24。
ホスト 100.65.1.111 がポート 443 で TCP SYN パケットを 100.65.0.200 に送信する場合、FortiGate がパケットを宛先に転送するときのパケットの送信元アドレス、宛先アドレス、および宛先ポートはどうなるでしょうか。

A. それぞれ 10.0.11.254、100.65.0.200、443
B. それぞれ 10.0.11.254、10.0.15.50、4443。
C. それぞれ100.65.1.ill、10.0.11.50、4443。

D. それぞれ 100.65.1.111、10.0.11.50、443。
Answer: C (メーッセージを残す**)**
展示品より:
VIP-WEB-SERVER という名前の VIP が WAN (ポート 2) 上に次のように設定されています。
外部IP: 100.65.0.200
マッピングされた（内部IP: 10.0.11.50
ポート転送が有効（TCP）
外部サービスポート: 443
IPv4ポートへのマッピング: 4443
受信ファイアウォール ポリシー Web_Server_Access は次のとおりです。
WAN（ポート2）からLAN（ポート4）へ
宛先: VIP-WEB-SERVER
サービス: HTTPS
NAT: 無効（ソースNATは適用されない）
パケットはどうなるのか
ホスト 100.65.1.111 は、TCP SYN dst-port 443 を 100.65.0.200 に送信します。
FortiGate が VIP を照合してトラフィックを内部サーバーに転送する場合、FortiGate は VIP に基づいて宛先 NAT (DNAT) を実行します。
ポリシー NAT が無効になっているため、送信元 IP は変更されません。
ソースは100.65.1.111のままです
宛先 IP は VIP によって変換されます。
宛先は10.0.11.50になります
宛先ポートは VIP ポート転送によって変換されます。
宛先ポートは4443になります
したがって、FortiGate がパケットを宛先 (内部サーバー) に転送する時点では、次のようになります。
送信元アドレス: 100.65.1.111
宛先アドレス: 10.0.11.50
宛先ポート: 4443

最新問題**: 35**
展示物を参照してください。

Network diagram



NAT IP pool configuration

	Name	External IP Range	Type	ARP Reply
	SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
	SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
	SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

	Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
	LAN (port4) → WAN (port2) 3							
	TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
	PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
	IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

展示には、ネットワークに接続された FortiGate デバイスの図と、IP プール構成およびファイアウォール ポリシー オブジェクトが表示されます。
WAN (ポート2)インターフェースにはIPアドレスがあります

100.65.0.101/24。
LAN ポート4）インターフェースにはIPアドレスがあります
10.0.11.254/24。
HQ-PC-1 (10.0.11.50) のユーザーが BR-FGT (100.65.1.111) の IP アドレスに ping を実行した場合、トラフィックのソース NAT (SNAT) にはどの IP アドレスが使用されますか?
A. 100.65.0.101
B. 100.65.0.49
C. 100.65.0.149
D. 100.65.0.99
Answer: D (メーッセージを残す**)**
図から、LAN (ポート 4) から WAN (ポート 2) への関連するファイアウォール ポリシーが 3 つあり、それぞれがソース NAT に異なる IP プールを使用しています。
TCPトラフィック
サービス: ALL_TCP
目的地: BR1-FGT
IP プール: SNAT プール → 100.65.0.49
PINGトラフィック
サービス: PING
宛先: すべて
IP プール: SNAT-Remote1 → 100.65.0.99
IGMPトラフィック
サービス: IGMP
宛先: すべて
IP プール: SNAT-リモート → 100.65.0.149
HQ-PC-1 (10.0.11.50) のユーザーが BR1-FGT (100.65.1.111) にpingを送信しています。FortiOS では、ポリシーのマッチングは送信元、宛先、サービスなどのフィールドに基づいて行われ、上から順に最初に一致したポリシーが適用されます。
このトラフィックはICMPエコー（ping）であるため、PINGトラフィック（サービスPING、宛先すべて）」というポリシーに一致します。このポリシーは、「SNAT-Remote1で動的IPプールを使用する」を明示的に使用しており、外部IPアドレスは100.65.0.99に設定されています。
したがって、この ping に使用される送信元 NAT IP は 100.65.0.99 です。

最新問題**: 36**
メンバー選択に有効な SD-WAN ルール戦略はどれですか? (3 つの回答を選択してください)
A. 負荷分散なしの最低コスト (SLA)
B. 負荷分散による手動
C. 負荷分散による最低品質 (SLA)
D. 負荷分散による最低コスト (SLA)
E. 負荷分散による最高品質
Answer: A,B,D (メーッセージを残す**)**
FortiOS 7.6管理者学習ガイドおよび公式ドキュメントによると、SD-WANルール（サービス）は、特定の条件に一致するトラフィックのパス選択を決定します。バージョン7.6では、これらの戦略が複数のメンバーインターフェースをどのように処理するかに関して、特別な柔軟性が提供されています。
まず、手動とロードバランシング（ステートメントB）は有効な構成です。手動戦略では、管理者はインターフェースを優先順位に基づいて順序付けますが、ロードバランシングのトグルを有効にすると、FortiGateは稼働中のすべてのメンバーにトラフィックを分散できます。

次に、最低コスト SLA）戦略が強化され、2つのモードがサポートされるようになりました。ロードバランシングオプションが無効になっている場合は、ロードバランシングなしの最低コスト SLA）戦略ステートメントA）として動作し、SLAを満たす最もコストの低い単一のリンクが選択されます。一方、トグルを有効にすると、ロードバランシングありの最低コスト SLA）戦略ステートメントD）として動作し、FortiGateは個々のコストに関係なく、SLAターゲットを満たすすべてのインターフェースにトラフィックを分散します。
ステートメント C と E は正しくありません。 最低品質」は認識されている SD-WAN 戦略ではなく、最高品質戦略は、具体的には単一の 最良」リンクに対する優先順位に基づく選択であるため、このモードを選択した場合、GUI で負荷分散トグルを使用できないことを意味します。

最新問題**: 37**
SSL VPN 環境で中間デバイスがトラフィックをブロックすることによって発生する接続の問題を分析しています。
問題を効果的に解決できる 2 つの方法はどれですか? (2 つ選択してください。)
A. IKE フラグメンテーションをオフにすると、大規模な証明書ネゴシエーションの問題を修正できます。
B. フラグメントのドロップや大規模な証明書の交換に関する問題を解決するには、IPsec を使用する必要があります。
C. SSL VPN トンネル モードを使用すると、ブロックされた ESP ポートおよび UDP ポート (500 または 4500) の問題を防ぐことができます。
D. SSL VPN トンネルを使用してハブアンドスポーク トポロジを構成し、ブロックされた UDP ポートをバイパスできます。
Answer: A,C (メーッセージを残す**)**
IKE フラグメンテーションを無効にすると、証明書ネゴシエーション中に中間デバイスが大きな断片化されたパケットをブロックすることによって発生する問題を解決するのに役立ちます。
SSL VPN トンネル モードを使用すると、HTTPS 経由のトラフィックがカプセル化され、IPsec で一般的に使用される ESP および UDP ポートのブロックがバイパスされます。

最新問題**: 38**
展示物を参照してください。

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32  kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions  in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions  in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

管理者は、HA クラスター上のパフォーマンス ステータス出力を 55 秒間観察しました。
どの FortiGate がプライマリですか?

A. HQ-NGFW-1 （パラメータmemory-failover-flip-timeout設定付き）
B. パラメータ優先度設定付きHQ-NGFW-2
C. パラメータオーバーライド設定付きのHQ-NGFW-1
D. パラメータmemory-failover-threshold設定を持つHQ-NGFW-2

Answer: (解答を表示する**)**

HQ-NGFW-1 の HA 構成から:

メモリベースのフェイルオーバーを有効にする
メモリフェイルオーバーしきい値を70に設定する
メモリフェイルオーバーモニター期間を50に設定する
メモリフェイルオーバーのサンプルレートを10に設定する
メモリフェイルオーバーフリップタイムアウトを60に設定する
オーバーライドを無効にする
優先度200を設定
パフォーマンス ステータスの出力から:
HQ-NGFW-1 のメモリ使用率は 90% です（設定されたしきい値 70% を大幅に上回っています）。HQ-NGFW-2 のメモリ使用率は約 48.7% です（しきい値を大幅に下回っています）。メモリベースのフェイルオーバーが FortiOS 7.6 で有効になっている場合の動作 メモリベースのフェイルオーバーを有効にすると、FortiGate はメモリ使用率を監視します。ユニットのメモリ使用量が、設定されたメモリフェイルオーバーしきい値を、設定されたメモリフェイルオーバー監視期間にわたって上回り続ける場合、クラスタはメモリ不足のユニットからフェイルオーバーをトリガーします。
閾値 = 70%
HQ-NGFW-1 は 90% なので、しきい値に違反しています。
監視期間 = 50 秒。
管理者は 55 秒間観察しました。これは 50 秒よりも長いため、フェイルオーバーをトリガーするのに十分な時間条件が満たされています。
メモリフェイルオーバーフリップタイムアウト 60 は、フェイルオーバーの決定後にロールの急速な変更 (フラッピング) を防ぐために使用されます。しきい値違反が監視期間中に継続すると、最初のフェイルオーバーの発生を防ぐことはできません。

最新問題**: 39**
管理者はNTurboをサポートするFortiGateモデルを管理します
NTurbo アクセラレーションはどのようにしてウイルス対策のパフォーマンスを向上させるのでしょうか?
A. フローベースの検査用。NTurbo は、IPS エンジンと FortiGate の入力および出力インターフェース間のトラフィックをリダイレクトするための専用データ パスを確立します。
B. フローベースの検査用。NTurbo は FortiGate デバイス上に 2 つの検査セッションを作成します。
C. プロキシベースの検査用。NTurbo はトラフィックをコンテンツ プロセッサにオフロードします。
D. プロキシベースの検査用。NTurbo はファイル全体をバッファリングし、ウイルス対策エンジンに送信します。
Answer: (解答を表示する**)**
FortiOS 7.6 管理ガイドおよび Fortinet ハードウェア アクセラレーション (NTurbo) のドキュメントによると、正解は A です。
NTurboとは（FortiOS 7.6 - 検証済み）
NTurboは、特定のFortiGateモデルで利用可能なハードウェアベースのアクセラレーション機能です。フローベース検査モードでの動作時に、ウイルス対策とIPSのパフォーマンスを向上させるように設計されています。
NTurbo は、次の間に高速で最適化されたデータ パスを作成することで機能します。
FortiGate 入力インターフェース
IPS/AVエンジン
FortiGate出力インターフェース
これにより、CPU の関与が最小限に抑えられ、パケット トラバーサルのオーバーヘッドが削減されます。
オプションAが正しい理由
A . フローベースの検査では、NTurbo は専用のデータ パスを確立し、IPS エンジンと FortiGate の入力および出力インターフェイス間のトラフィックをリダイレクトします。
NTurbo の動作は、次のように文書化されています。
NTurboはフローベースの検査にのみ適用されます
IPSとウイルス対策スキャンを高速化します

不要な処理ステップをバイパスする専用の高速パスを作成します。これにより、スループットが大幅に向上し、待ち時間が短縮されます。この説明は、Fortinet による NTurbo の公式説明と一致しています。
他の選択肢が間違っている理由
B . NTurboは2つの検査セッションを作成する
不正解です。NTurbo はセッションを複製せず、パケット パスを最適化します。
C . NTurboはトラフィックをコンテンツプロセッサ（プロキシベース）にオフロードします。
不正解です。NTurbo はプロキシベースの検査には適用されず、コンテンツプロセッサにオフロードされません。
D . NTurboはファイル全体をバッファリングしてから、ウイルス対策エンジンに送信します。不正解です。ファイル全体をバッファリングするのはプロキシベースの動作であり、NTurboの動作ではありません。

最新問題**: 40**
オートメーションステッチの特徴を説明する 2 つの記述はどれですか? (2 つの回答を選択してください)
A. アクションは、セキュリティ ファブリックに含まれるデバイスのみに関係します。
B. オートメーション ステッチには複数のトリガーを設定できます。
C. 複数のアクションを並行して実行できます。
D. トリガーには外部コネクタが含まれる場合があります。
Answer: C,D (メーッセージを残す**)**
FortiOS 7.6管理ガイドおよびセキュリティファブリックのドキュメントによると、自動化ステッチは、ネットワーク全体のセキュリティおよびシステムイベントへの対応を自動化するように設計されています。これらのステッチの中心的な特徴は、アクション実行の柔軟性です。具体的には、複数のアクションを並行して実行できます（ステートメントC）。システムは、アクション間の遅延を設定可能なシーケンシャル実行を可能にしますが、デフォルトの動作または設定オプションでは、Webhookのトリガーやホストの隔離と同時にメール通知を送信するなど、同時対応が可能です。
さらに、トリガーには外部コネクタが関与する場合があります（ステートメントD）。多くのトリガーはFortiGateのローカルなトリガー（再起動やログイベントなど）ですが、セキュリティファブリックにより、FortiGateはFortiAnalyzer、FortiSIEM、FortiClient EMSなどの外部コンポーネントからのイベントを監視し、対応することができます。例えば、FortiAnalyzerのイベントハンドラは、ルートFortiGateのステッチのトリガーとして機能することができます。ステートメントAは誤りです。アクションは、ファブリックの内部デバイスではないAWS LambdaやSlackなどの外部システムをターゲットにすることができるためです。
ステートメント B は正しくありません。各オートメーション ステッチは通常、単一のトリガーによって定義されますが、そのトリガー自体は広範囲に及ぶ可能性があります (例: 「任意のセキュリティ評価通知」)。

最新問題**: 41**
ネットワーク接続なしで FortiGate CLI への管理アクセスを許可する方法はどれですか?
A. CLI コンソール ウィジェット
B. シリアルコンソール
C. Telnetコンソール
D. SSHコンソール
Answer: B (メーッセージを残す**)**
シリアルコンソールは、ネットワーク接続を必要とせずにFortiGate CLIに直接物理的にアクセスできるようにします。シリアルケーブルを使用してFortiGateのコンソールポートに接続するため、ネットワークインターフェースがダウンしていたり、設定が誤っていたりする場合でも、管理者は初期設定、復旧、トラブルシューティングを実行できます。

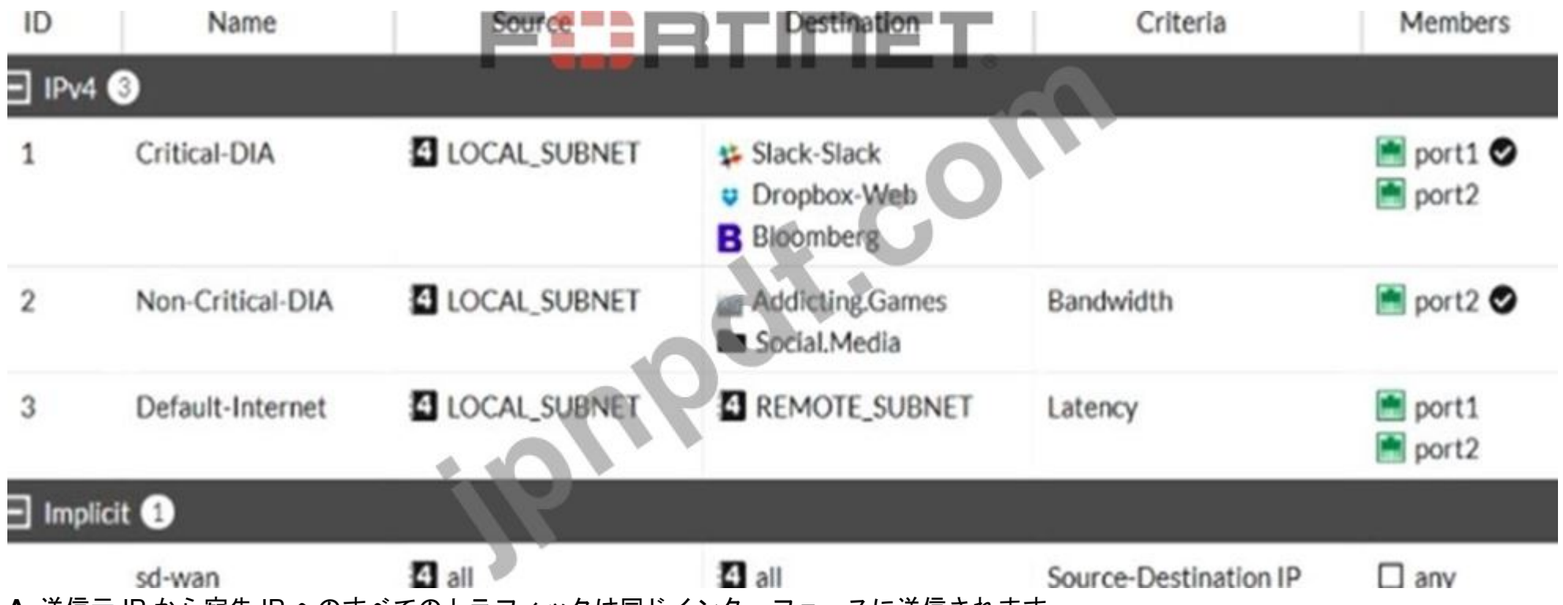
最新問題**: 42**
管理者は、FGCP プロトコルを使用して HA クラスターを形成したいと考えています。
管理者は、両方のメンバーが満たしていることを確認する必要がある 2 つの要件はどれですか? (2 つ選択してください。)
A. 同じ HA グループ ID を持つ必要があります。
B. 同じサブネット内にハートビート インターフェイスが必要です。

C. 構成された VDOM の数は同じである必要があります。
D. ハードドライブ構成は同じである必要があります。
Answer: (解答を表示する**)**
同じ HA グループ ID と同じハード ドライブ構成が必要です。

最新問題**: 43**
ネットワーク管理者はウイルス対策を有効にし、ファイアウォールポリシーでSSLインスペクションプロファイルを選択しました。EICARテストファイルをHTTP経由でダウンロードすると、FortiGateはウイルスを検出し、ファイルをブロックしました。同じファイルをHTTPS経由でダウンロードすると、FortiGateはウイルスを検出せず、ファイルをブロックせず、ダウンロードを許可しました。
管理者は、トラフィックが設定されたファイアウォールポリシーと一致していることを確認しました。FortiGateによるウイルス検出に失敗した2つの理由は何ですか？ 2つ選択してください。）
A. ウェブサイトは SSL 検査の対象外です。
B. ブラウザは FortiGate 自己署名 CA 証明書を信頼していません。
C. 選択された SSL 検査プロファイルでは証明書検査が有効になっています。
D. El CAR テスト ファイルがプロトコル オプションのサイズ超過制限を超えています。
Answer: A,C (メーッセージを残す**)**
証明書の検査は詳細な SSL 検査ではないため、パケットは暗号化されているため検査は行われません。
https サイトが試験リストに含まれている場合、それは正当な理由です。

最新問題**: 44**
FortiGate デバイスが節約モードに入るときに正しい 2 つのステートメントはどれですか? (2 つ選択してください。)
A. FortiGate はシステム操作を完全に停止し、使用可能なリソースを回復するには再起動が必要です。
B. IPS のフェールオープン グローバル設定が有効になっている場合、FortiGate は IPS 検査なしでパケットの送信を継続します。
C. FortiGate は、隔離などの重要なセキュリティ アクションを引き続き実行します。
D. FortiGate は設定の変更を拒否します。
Answer: B,D (メーッセージを残す**)**

最新問題**: 45**
図を参照してください。SD-WANは、どのSD-WANルールにも一致しないトラフィックを分散するためにどのアルゴリズムを使用しますか？



ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

A. 送信元 IP から宛先 IP へのすべてのトラフィックは同じインターフェースに送信されます。
B. トラフィックは、遅延が最も低いリンクに送信されます。
C. トラフィックは、各インターフェースを通過するセッション数に基づいて分散されます。
D. 送信元IPからのすべてのトラフィックは同じインターフェースに送信されます
Answer: A (メーッセージを残す)
定義されたSD-WANルールのいずれにも一致しないトラフィックには、デフォルトの暗黙的なSD-WANルールが適用されます。デフォルトでは、FortiGateは 「送信元IP-宛先IPベース」アルゴリズムを使用します。つまり、特定の送信元IPから特定の宛先IPへのすべてのトラフィックは同じインターフェースを介して送信されます。
これにより、同じ送信元 IP アドレスと宛先 IP アドレス間のトラフィックに一貫したパスが使用されるようになります。

最新問題**: 46**
マルチ WAN セットアップで FortiGate を構成する場合、管理者がインターフェースでセッション保存を有効にするのはなぜですか?
A. WANリンクに障害が発生したときに、FortiGateがすべてのアクティブセッションのインターフェースを動的に変更できるようにする
B. ソースNATが有効になっていないすべてのセッションが常にプライマリWANリンクを使用するようにするには
C. WANリンクが変更されたときにユーザーに再度認証を強制することでセキュリティを向上させる
D. ルート変更が発生しても、既存のSSL VPN接続が同じインターフェース上に維持されるようにするため
Answer: D (メーッセージを残す)
セッション保存により、SSL VPN などのアクティブなセッションが元のインターフェイスに結び付けられ、WAN ルートの変更時に中断が防止されます。

最新問題**: 47**

添付資料を参照してください。管理者は、HAクラスタのパフォーマンスステータス出力を55秒間観察しました。

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
```

```
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32  kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions    in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions  in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

どの FortiGate がプライマリですか?

A. パラメータmemory-failover-threshold設定を持つHQ-NGFW-2

B. パラメータ優先度設定付きHQ-NGFW-2

C. HQ-NGFW-1（パラメータmemory-failover-flip-timeout設定付き）

D. パラメータオーバーライド設定付きHQ-NGFW-1

Answer: (解答を表示する**)**

設定されたメモリフェイルオーバーのしきい値は70%ですが、FW-1は90%で動作しています。監視期間は50秒に設定されていますが、質問には管理者が出力を55秒間監視したと記載されています。これは、FW-1が設定された監視期間を超えて70%のしきい値を超えている一方で、FW-2のメモリ使用率は70%を下回っていることを意味します。

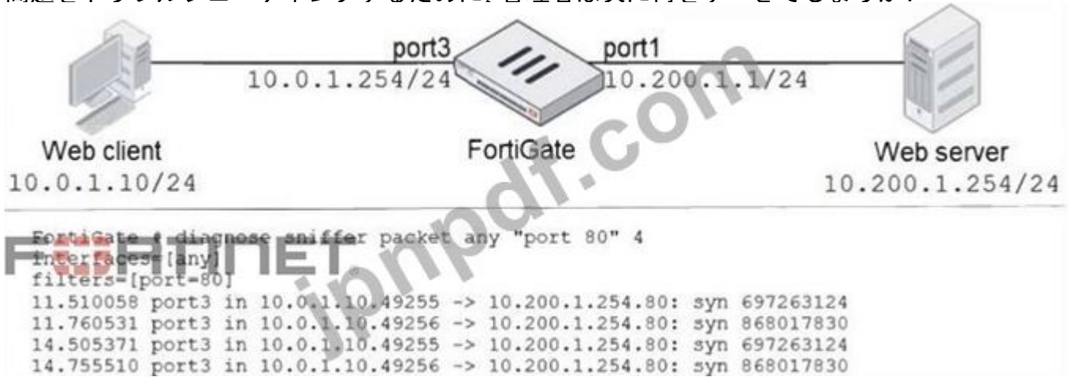
最新問題**: 48**

別紙を参照してください。FortiGuard接続に関する正しい記述は2つありますか？（2つ選択してください。）

```
FortiGate # diagnose debug rating
Locale        : English

Service       : Web-filter
Status:       : Enable
License       : Contract
\
Num. of servers     : 1
Protocol            : https
Port                : 8888
Anycast             : Disable
Default servers     : Not included

-=- Server List (Wed Sep 20 09:22:42 2023) -=-

IP          Weight  RTT  Flags TZ  FortiGuard-requests Curr Lost Total Lost Updated Time
10.0.1.241  -244    2    I     0          122              0           0   Wed Sep 20 09:21:55 2023
```

A. FortiGate は FortiGuard 通信にデフォルトのポートを使用しています。
B. FortiGate は DNS ルックアップを使用して FortiGuard サーバーを識別しました。
C. 失敗したパケットの数が増えると重みが増加します。
D. FortiGuard Server と通信するために、信頼性の低いプロトコルを設定できます。
Answer: (解答を表示する**)**
FortiGuardウェブフィルタリング、DNSフィルタリング、アンチスパムサービス。fortiguard.netはUDPポート53または8888で独自のプロトコルを使用し、securewf.fortiguard.netはポート443、53、または4448でHTTPSを使用します。
8888。
重みの値はサーバーの信頼性を反映します。パフォーマンスが良好であれば重みは減少し、パケットロスや障害が増加すると重みは増加します。つまり、重みが高いほど障害発生率が高いことを意味します。

最新問題**: 49**
図を参照してください。図に示されているネットワークでは、WebクライアントはHTTP Webサーバーに接続できません。管理者はFortiGate内蔵スニファーを実行し、図に示されている出力を取得します。
問題をトラブルシューティングするために、管理者は次に何をすべきでしょうか?



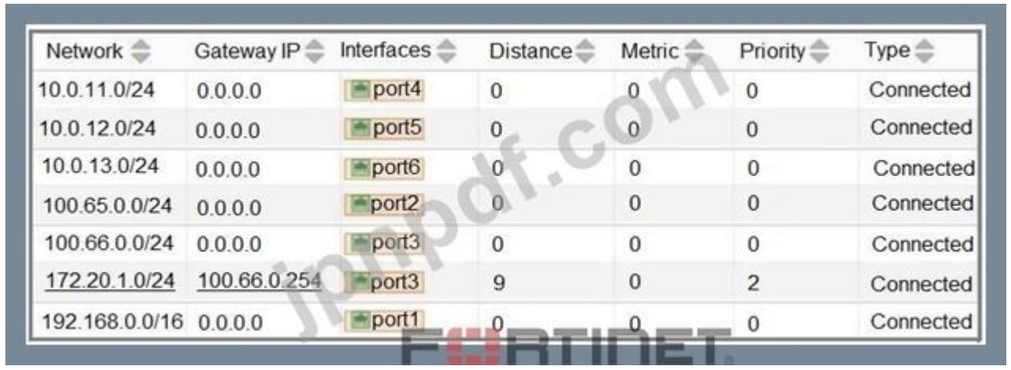
A. デバッグフローを実行します。
B. ポート1に接続された外部スニファーを使用してトラフィックをキャプチャします。
C. 今回はフィルター「host 10.0.1.10」を使用して、FortiGate で別のスニファーを実行します。
D. Web サーバー上でスニファーを実行します。

Answer: A (メッセージを残す)
スニファーの出力を見ると、Webクライアントからのパケットが FortiGateに到達し、Webサーバーに転送されていることがわかりますが、Webサーバーが応答している兆候はありません。この問題をトラブルシューティングするには、デバッグフローを実行することでトラフィックパスを分析し、問題の発生箇所を特定することができます。例えば、ファイアウォールポリシーやルート設定に問題があり、サーバーが正しく応答しないなどの原因となっている可能性があります。

最新問題: **50**
管理者は、デフォルト設定を使用して、FortiGuard サーバーを FortiGate 上の DNS サーバーとして構成します。
FortiGuard サーバーへの DNS 接続に関して正しいのは何ですか?
A. DNS over TLS を使用します。
B. DNS over HTTPS を使用します。
C. UDP 8888 を使用します。
D. UDP 53 を使用します。
Answer: A (メッセージを残す)
DNSにFortiGuardサーバーを使用する場合、FortiOSはデフォルトでDNS over TLS（DoT）を使用してDNSトラフィックを保護します。新しいFortiGuard DNSサーバーがプライマリサーバーとセカンダリサーバーとして追加されました。

最新問題: **51**
プロファイルベースの次世代ファイアウォール (NGFW) として構成されている場合、FortiGate はアプリケーション プロファイルにどの検査モードを使用しますか?
A. 証明書検査
B. フローベースの検査
C. プロキシベースの検査
D. 完全なコンテンツ検査
Answer: B (メッセージを残す)
アプリケーション制御は、プロキシベースおよびフローベースのファイアウォールポリシーで設定できます。ただし、アプリケーション制御ではフローベースの検査を行うIPSエンジンが使用されるため、検査は常にフローベースになります。
最新問題: **52**
ネットワーク管理者は、海外に出張する営業担当者のために IPsec VPN トンネルを構成しています。
管理者はどの IPsec ウィザード テンプレートを適用する必要がありますか?
A. ハブアンドスポーク
B. サイト間
C. リモートアクセス
D. ダイヤルアップユーザー
Answer: C (メッセージを残す)
リモートアクセスIPsecウィザードテンプレートは、出張中の従業員など、遠隔地から接続する個々のユーザー向けに使用します。このテンプレートは、FortiGateをIPsec VPNサーバーとして動作するように設定し、FortiClientなどのリモートクライアントが海外から安全に接続して社内ネットワークリソースにアクセスできるようにします。

最新問題: **53**
ルーティング テーブルを示す展示を参照してください。

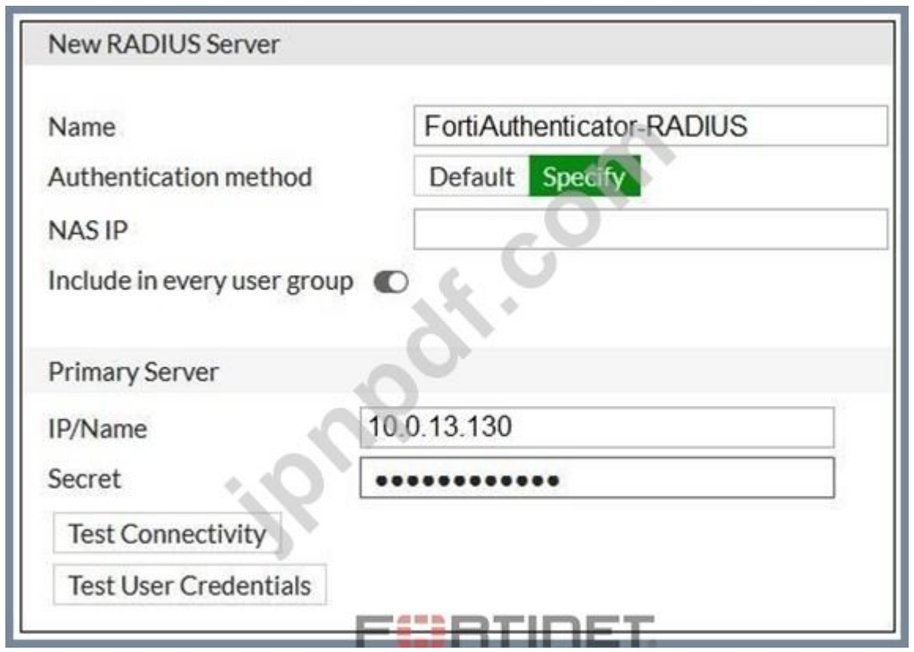


Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Connected
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

管理者は、サブネット 172.20.1.0/24 へのトラフィックがポート 2 のみを経由してルーティングされるように、新しい静的ルートを作成したいと考えています。
管理者がこの目的を達成するために使用できる 2 つの基準は何ですか? (2 つ選択してください。)
A. 新しい静的ルートの距離を 9 に設定する必要があります。
B. ポート3 を経由する既存の静的ルートの距離は 11 に設定する必要があります。
C. 新しい静的ルートの優先度は 3 に設定する必要があります。
D. 新しい静的ルートのメトリックは 1 に設定する必要があります。
Answer: B,C (メーッセージを残す)
現在、サブネット 172.20.1.0/24 は、距離 9、優先度 2 でポート 3 経由でルーティングされています。ポート 2 経由のルーティングを強制するには、管理者は次の操作を行う必要があります。
- ポート 3 経由の既存ルートの距離を増やし (たとえば、11 に)、優先度を下げます。
- 距離が等しい場合に現在のポート 3 ルートを上書きするように、ポート 2 の新しい静的ルートをより高い優先度値 (例: 3) で設定します。

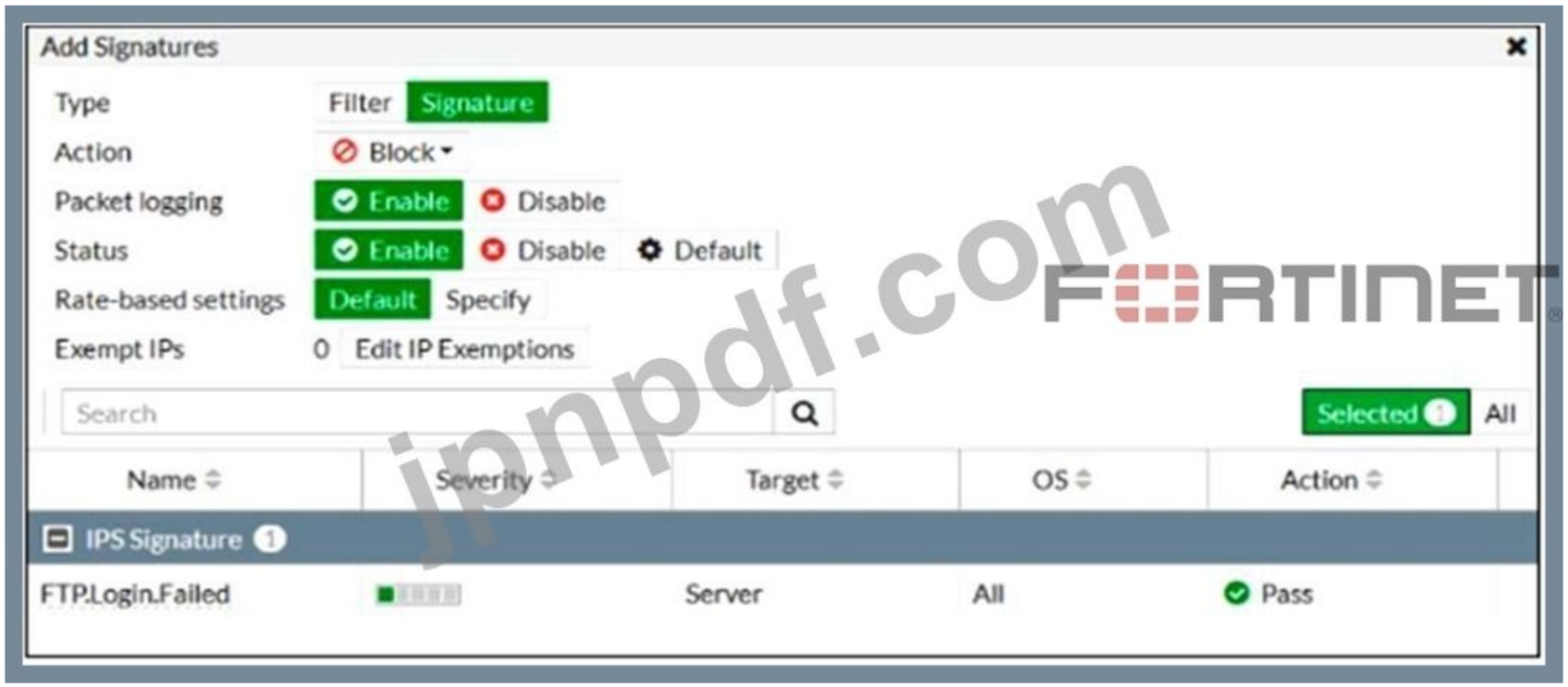
最新問題**: 54**
FortiGate デバイスの HA クラスター ハートビート IP アドレスの 2 つの特性は何ですか?
(2つ選択してください。)
A. ハートビート インターフェイスには、手動で割り当てられた仮想 IP アドレスがあります。
B. ハートビート IP アドレスは、クラスター メンバーを区別するために使用されます。
C. クラスタ内のプライマリデバイスのハートビートインターフェースには常にIPアドレスが割り当てられます
169.254.0.1。
D. FortiGate デバイスがクラスターに参加またはクラスターから離脱すると、ハートビート IP アドレスが変更されます。
Answer: B,D (メーッセージを残す)
FGCPは、仮想HAハートビートインターフェース（port_ha）およびvsys_haと管理VDOM間のVDOM間リンクインターフェースに、169.254.0.x範囲のリンクローカルIPv4アドレス（RFC 3927参照）を使用します。メンバーがHAクラスタに参加すると、各メンバーのハートビートインターフェース（port_ha）には、169.254.0.1から169.254.0.63/26の範囲のIPアドレスが割り当てられます。HA VDOM間リンクインターフェース（havdlink0およびhavdlink1）には、169.254.0.xの範囲のIPアドレスが割り当てられます。
169.254.0.65 から 169.254.0.66/26 へ。
仮想ハートビートインターフェースに割り当てられるIPアドレスは、メンバーのシリアル番号の優先度によって決まります。シリアル番号が大きいほど優先度が高くなり、serialno_prioの値は低くなります。

最新問題**: 55**
RADIUS サーバーの構成が記載されている展示を参照してください。



管理者が新しいRADIUSサーバーの設定を追加しました。設定中に、管理者は 「すべてのユーザーグループに含める」オプションを有効にしました。
RADIUS 構成ですべてのユーザー グループに含めるを有効にするとどのような影響がありますか?
A. このオプションは、RADIUS サーバーと、そのサーバーに対して認証できるすべてのユーザーを、すべての FortiGate ユーザー グループに配置します。
B. このオプションは、RADIUS サーバーと、そのサーバーに対して認証できるすべてのユーザーをすべての RADIUS グループに配置します。
C. このオプションは、FortiGate 上の LDAP サーバーに使用されるグループを含む、すべてのユーザーをすべての RADIUS ユーザー グループに配置します。
D. このオプションは、認証に必要なすべての FortiGate ユーザーとグループを RADIUS サーバー (この場合は FortiAuthenticator) に配置します。
Answer: (解答を表示する**)**
RADIUS設定で 「すべてのユーザーグループに含める」を有効にすると、RADIUSサーバーがすべてのFortiGateユーザーグループに自動的に追加されます。その結果、RADIUSサーバーに対して認証に成功したユーザーは、手動で割り当てる必要がなく、すべてのFortiGateユーザーグループのメンバーになります。ただし、慎重に管理しないと、意図せず過剰なアクセスを許可してしまう可能性があります。

最新問題**: 56**
展示品を参照してください。



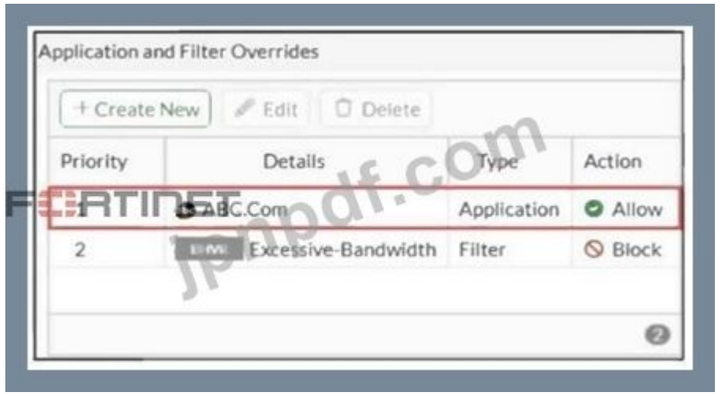
図に示されている侵入防止システム (IPS) プロファイル署名設定を確認します。
FTP.Login.Failed 署名を IPS センサー プロファイルに追加すると、どのような結論になりますか?

A. シグネチャに一致するトラフィックは許可され、ログに記録されます。
B. 署名設定ではカスタム評価しきい値が使用されます。
C. 署名設定には他の署名のグループが含まれます。
D. シグネチャに一致するトラフィックは、黙ってドロップされ、ログに記録されます。

Answer: D (メーッセージを残す**)**

エントリに含まれるシグネチャのいずれかに一致するトラフィックを黙ってドロップするには、[ブロック] を選択します。
つまり、このシグネチャのデフォルトのアクションは 許可」ですが、管理者はそれを明示的に上書きしてブロックアクションを設定しています。デフォルトのアクションを使用するには、設定を次のようにする必要があります。
'デフォルト'。

最新問題**: 57**
添付資料を参照してください。管理者はABC.Comのアプリケーションシグネチャに対してアプリケーションオーバーライドを設定し、アクションを 許可」に設定しました。このアプリケーション制御プロファイルは、すべての送信トラフィックをスキャンするファイアウォールポリシーに適用されています。ファイアウォールポリシーではログ記録が有効になっています。設定をテストするため、管理者はABC.Comのウェブサイトに複数回アクセスしました。



ABC.Com のセキュリティ ログにログが生成されないのはなぜですか?

A. ABC.Com タイプはフィルターではなくアプリケーションとして設定されています。

B. ABC.Com はアプリケーション プロファイル下に設定されており、Web フィルタ プロファイルとして設定する必要があります。

C. ABC.Com アクションが許可に設定されています。

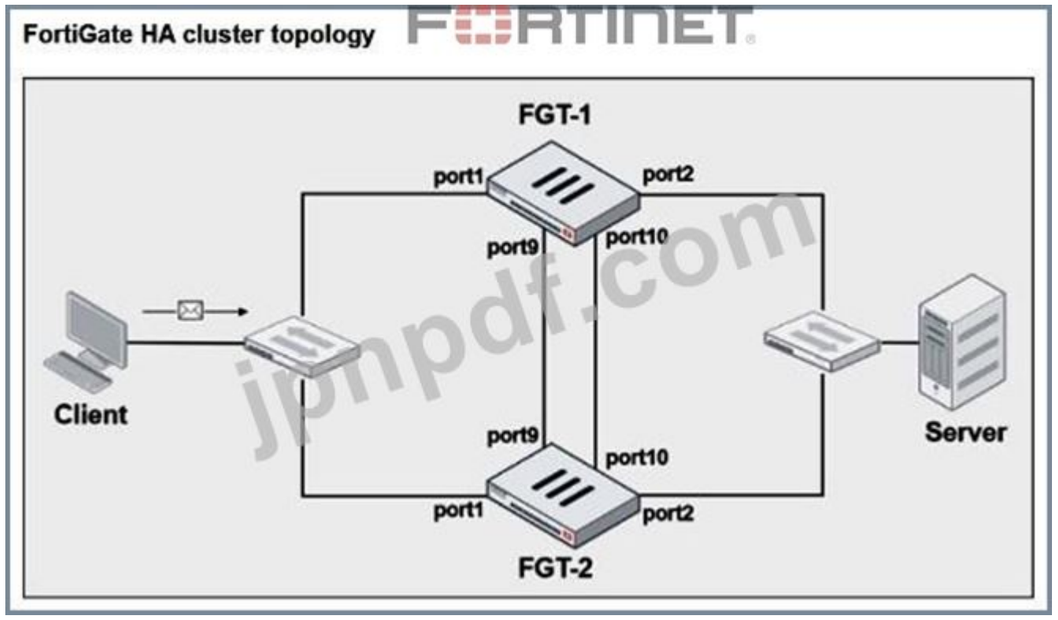
D. ABC.Com は、過剰な帯域幅のカテゴリに該当します。

Answer: (解答を表示する**)**

アプリケーション オーバーライドでアクションが [許可] に設定されている場合、このオーバーライドに一致するトラフィックは、より詳細な検査とブロックをバイパスするため、セキュリティ ログを生成せずに許可されます。

最新問題**: 58**

展示物を参照してください。



Current HA status

```
# get system ha status
...
Configuration Status:
    FGVM010000064692(updated 4 seconds ago): in-sync
    FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
    FGVM010000065036(updated 4 seconds ago): in-sync
    FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary     : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary   : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

```
FGT-1
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override disable
    set priority 90
    set monitor port3

FGT-2
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override enable
    set priority 110
    set monitor port3
```

FGT-1 および FGT-2 は、図に示す HA 構成コマンドで更新されます。

HA クラスターで期待される結果は何でしょうか?

A. FGT-2 はオーバーライド有効設定を持ち、FGT-1 よりも優先度が高いため、プライマリとして引き継ぎます。

B. FGT-1 はオーバーライド無効化設定を FGT-2 と同期します。

C. オーバーライド設定はすべての HA メンバーで一致する必要があるため、HA クラスターは同期されなくなります。

D. FGT-2 の優先度が低いため、FGT-1 がプライマリのままになります。

Answer: A (メーッセージを残す)

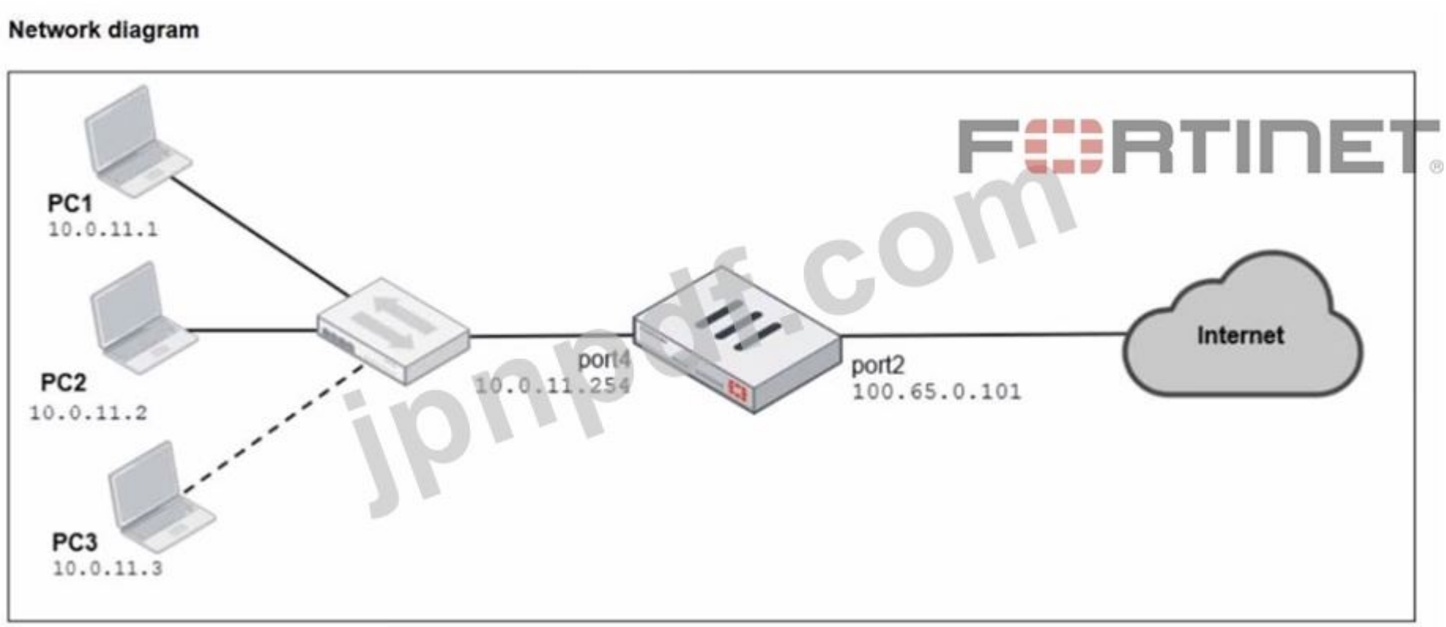
オーバーライドを有効にすると、デバイス優先度が最も高いプライマリユニットが常にプライマリユニットになります。プライマリユニットの選択に影響を与える可能性のあるイベントが発生するたびに、クラスタはネゴシエーションを行います。例えば、オーバーライドが有効になっている場合、クラスタユニットのデバイス優先度が変更されたり、クラスタに新しいユニットが追加されたりすると、クラスタは再ネゴシエーションを行います。
オーバーライドとプライマリユニットの選択
オーバーライドを有効にすると、プライマリユニットの選択順序が変更されます。以下に示すように、オーバーライドを有効にすると、プライマリユニットの選択では、デバイスの優先度が、使用期間とシリアル番号よりも優先されます。つまり、あるクラスタユニットでデバイスの優先度を高く設定した場合、オーバーライドを有効にすると、そのクラスタユニットの使用期間とシリアル番号が他のクラスタユニットよりも低くても、そのクラスタユニットがプライマリユニットになります。

最新問題**: 59**
管理者は、特定の期間内にシグネチャセットを一定回数トリガーするトラフィックをブロックするようにIPSセンサーを設定したいと考えています。この目的を達成するにはどうすればよいでしょうか？
A. IPS グループ シグネチャを使用し、レート モードを 60 に設定します。
B. 定期的なフィルタ オプションとともに IPS パケット ログ オプションを使用します。
C. IPS シグネチャ、レート モード定期オプションを使用します。
D. IPS フィルター、レート モード定期オプションを使用します。
Answer: D (メーッセージを残す**)**
FortiOS 7.6 では、管理者が定義された時間枠内に IPS シグネチャが特定の回数トリガーされた後にのみトラフィックをブロックしたい場合、レートベースの設定を持つ IPS フィルターを使用してこれを行う必要があります。
選択肢Dが正しい理由
IPS フィルターを使用すると、管理者は次のような属性に基づいてシグネチャを一致させることができます。
重大度
プロトコル
CVE
署名ID
IPS フィルターは、以下を使用してレートベースのアクションをサポートします。
レートモード定期刊行物
レートカウント
レート期間
レートモード定期の場合、FortiGateは次のようになります。
署名がトリガーされた回数をカウントします
定められた期間内
しきい値を超えると、設定されたアクション (ブロックなど) が適用されます。これは要件に直接一致します。
「特定の期間内にシグネチャ セットをトリガーするトラフィックをブロックします。」他のオプションが間違っている理由 A . IPS グループ シグネチャ、レート モード 60 の設定 グループ シグネチャでは、必要な期間ごとのレートベースのブロッキング ロジックが提供されません。
B . IPSパケットログオプション
ログ記録ではブロック動作は強制されません。
C . IPSシグネチャ、レートモード定期オプション
レートベースの制御は、個々のシグネチャ定義に直接適用されるのではなく、IPS フィルターを介して適用されます。

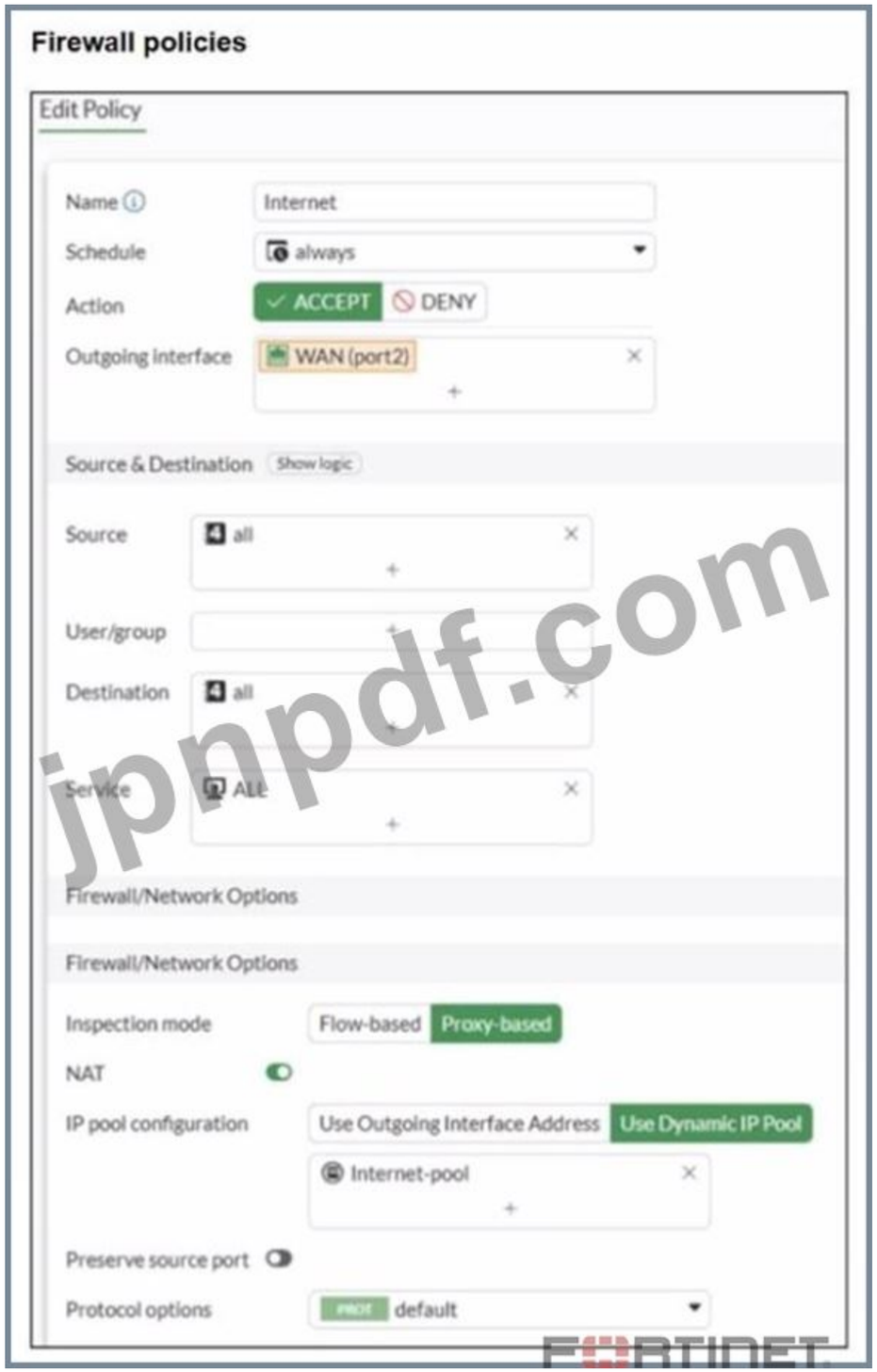
最新問題**: 60**
FortiGate が SSL/SSH 完全検査を実行するときに、無効な証明書を検出した場合の対応方法を決定できます。

無効な証明書を検出したときに FortiGate が実行できる有効なアクションはどれですか (3 つ選択してください)。
A. 許可する
B. 信頼して許可
C. 許可と警告
D. ブロック
E. ブロックと警告
Answer: A,B,D (メーッセージを残す**)**
上記のいずれかの理由で証明書が失敗した場合は、次のいずれかのアクションを設定できます。
* 信頼できないサイトを保持して許可: FortiGate は Web サイトを許可し、ブラウザが実行するアクションを決定できるようにします。
FortiGate は証明書を信頼できないものとして扱います。
* ブロック: FortiGate はサイトのコンテンツをブロックします。
* 信頼と許可: FortiGate は Web サイトを許可し、証明書を信頼できるものとして扱います。

最新問題**: 61**
展示物を参照してください。




Dynamic IP pool
Edit Dynamic IP Pool
Name
Internet-pool
Comments
Write a comment...
0/255
Type
One-to-One
External IP Range
100.65.0.110-100.65.0.111
ARP Reply



ネットワークに接続された FortiGate デバイスの図と、FortiGate デバイス上のファイアウォール ポリシーと IP プール構成が表示されます。
2台のPC（PC1とPC2）はFortiGateの背後に接続されており、インターネットに正常にアクセスできます。しかし、管理者がネットワークに3台目のPC（PC3）を追加すると、そのPCはインターネットに接続できな

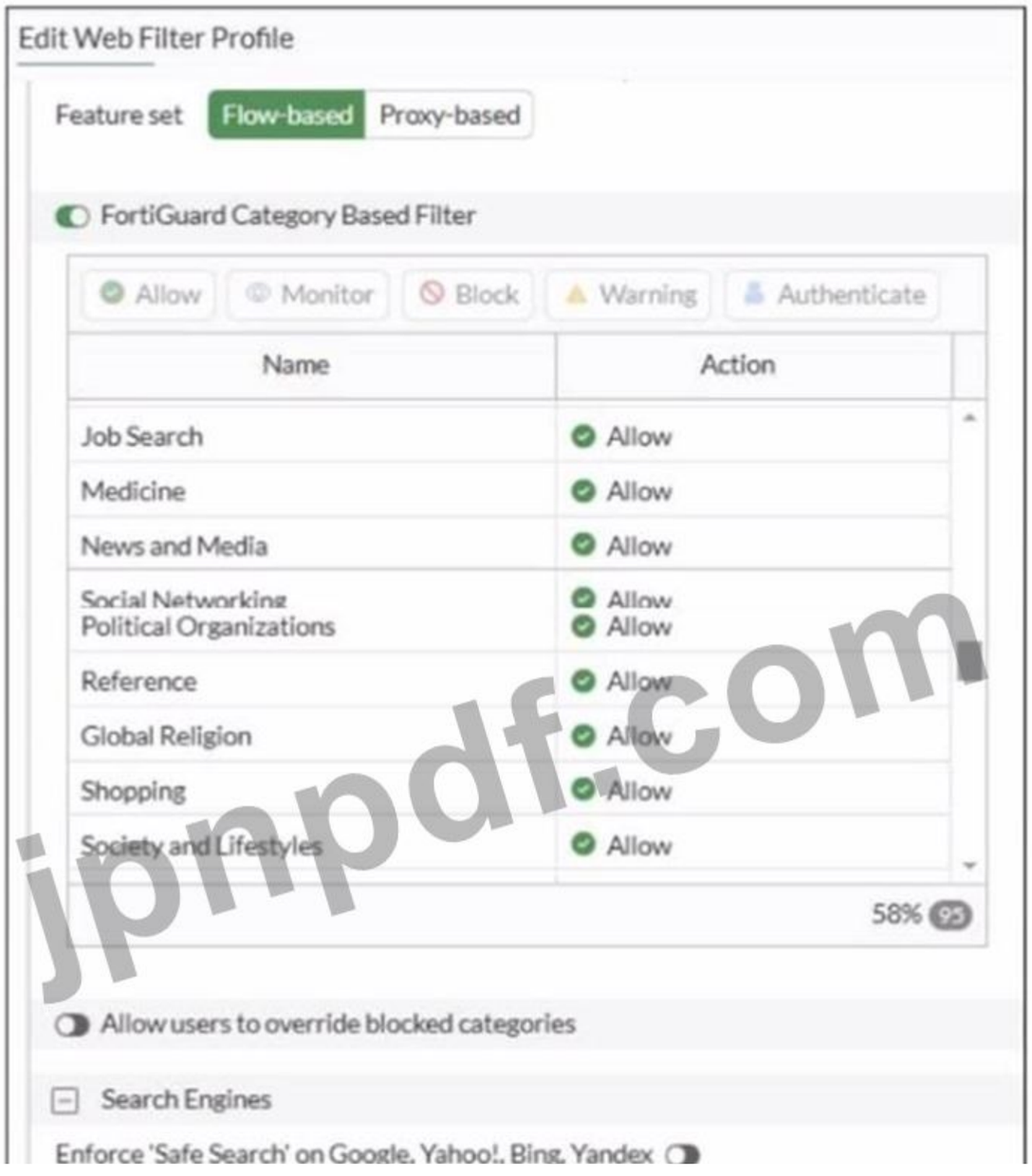
くなります。
展示に示されている情報に基づいて、管理者が PC3 の接続の問題を解決するために使用できる 2 つの構成オプションはどれですか? (2 つ選択してください。)
A. システム設定で、複数のインターフェース ポリシーを有効にします。
B. IP プール構成で、end ipto 100.65.0.112 を設定します。
C. ファイアウォール ポリシーで、CLI を使用して match-vip を有効に設定します。
D. IP プール構成で、タイプをオーバーロードに設定します。
Answer: B,D (メーッセージを残す**)**
展示品より:
ファイアウォール ポリシーでは NAT が有効になっており、動的 IP プールを使用するように構成されています。
選択した IP プール (インターネット プール) は次のように構成されます。
タイプ: 1対1
外部 IP 範囲: 100.65.0.110-100.65.0.111 (パブリック IP は 2 つのみ)
PC1とPC2は、1対1のNATマッピングごとにプールからパブリックIPアドレスを1つずつ消費するため、インターネットにアクセスできます。PC3が追加されると、プールに3つ目のパブリックIPアドレスがないため、FortiGateはPC3に1対1のマッピングを割り当てることができず、セッションは失敗します。
ここでの FortiOS の動作は標準です。1 対 1 の IP プールでは、使用可能なプール サイズによって、同時に変換できる異なる内部ソースの数が制限されます (割り当てとセッションによって異なります)。また、IP が 2 つしかないプールでは、変換が必要な 3 つの個別のホストを確実にサポートできません。
したがって、管理者は次の 2 つの有効な方法でこれを修正できます。
B. IPプール設定で、end ipを100.65.0.112に設定します。
これにより、追加のパブリック IP アドレスが追加されてプールが拡張され、3 つのパブリック IP (.110、.111、.112) が使用可能になるため、PC3 に 1 対 1 NAT のアドレスを割り当てることができます。
D . IP プール構成で、タイプをオーバーロードに設定します。
プールタイプをオーバーロードに変更すると、PAT（多対一が有効になり、複数の内部ホスト（PC1、PC2、PC3）が異なる送信元ポートを使用してプールアドレスを共有できるようになります。これにより、1対1プールに固有の「内部ホストごとに1つのパブリックIP」という制限がなくなります。
他のオプションが正しくない理由:
A . 複数インターフェース ポリシーは IP プールの枯渇とは無関係であり、NAT 割り当て制限を解決しません。
C . match-vip は、宛先 NAT/仮想 IP の使用に関する VIP マッチング動作に影響し、PC3 の障害の原因となるソース NAT プールの不足には対処しません。

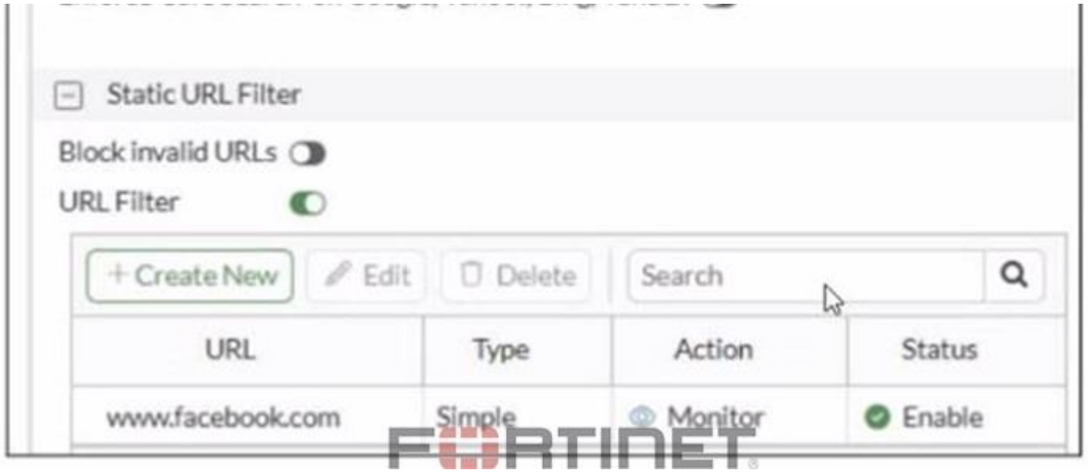
最新問題**: 62**
SSL VPN 環境で中間デバイスがトラフィックをブロックすることによって発生する接続の問題を分析しています。
問題を効果的に解決できる 2 つの方法はどれですか? (2 つ選択してください。)
A. IKE フラグメンテーションをオフにすると、大規模な証明書ネゴシエーションの問題を修正できます。
B. フラグメントのドロップや大規模な証明書の交換に関する問題を解決するには、IPsec を使用する必要があります。
C. SSL VPN トンネル モードを使用すると、ブロックされた ESP ポートおよび UDP ポート (500 または 4500) の問題を防ぐことができます。
D. SSL VPN トンネルを使用してハブアンドスポーク トポロジを構成し、ブロックされた UDP ポートをバイパスできます。
Answer: C,D (メーッセージを残す**)**

このトレーニングでは基本的に、中間デバイスによって問題が発生する状況において、IPSec VPN よりも FortiGate の SSL VPN の利点を指摘することを目的としています。
IPsec は ESP と UDP 500 および 4500 を使用するため、これらがブロックされている場所では、デフォルトで HTTPS (443) と TLS (両方とも TCP) を使用するため、SSL VPN トンネル モードが有効になります。
また、UDP ポートがブロックされている場合でも、SSL VPN は UDP を使用しないため有効です (トンネル モードのハブ アンド スポーク)。

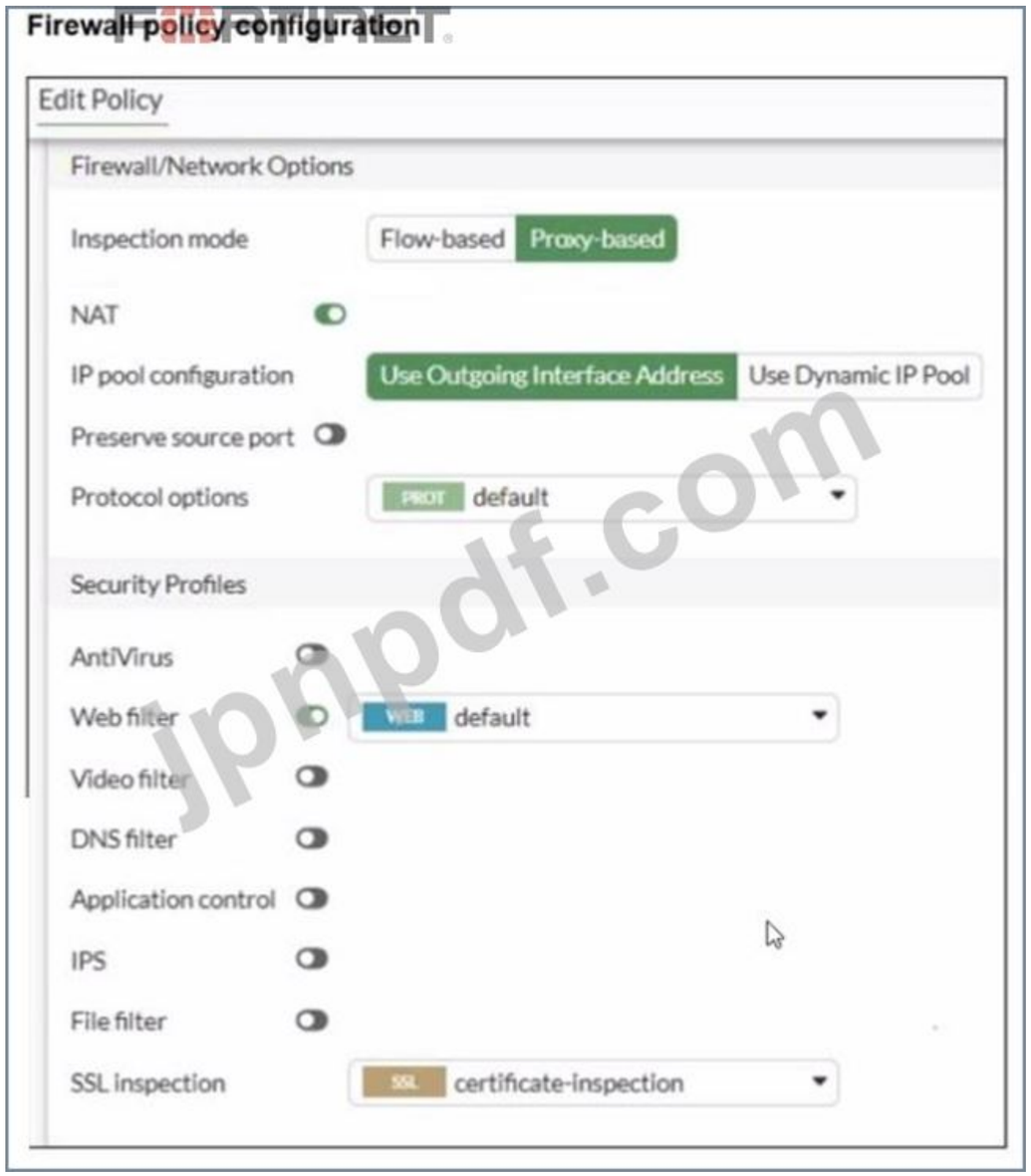
最新問題: **63**
展示物を参照してください。

Web filter profile configuration




Static URL Filter
Block invalid URLs
URL Filter
+ Create New
Edit
Delete
Search
URL
Type
Action
Status
www.facebook.com
Simple
Monitor
Enable

Firewall policy configuration



Web フィルタ プロファイル構成とファイアウォール ポリシー構成が表示されます。
www.facebook.com にアクセスしようとしていますが、FortiGuard Web フィルタリング ブロック ページにリダイレクトされます。
展示物に基づいて、問題の原因は何でしょうか?
A. Web 評価オーバーライド構成が正しくありません。
B. Web フィルタ プロファイルの機能セットが正しく構成されていません。
C. ファイアウォール ポリシー検査モードが正しくありません。
D. www.facebook.com. の場合、URL フィルター アクションが正しくありません。
Answer: (解答を表示する**)**
展示品より:
Web フィルタ プロファイルは、機能セット = フローベースで構成されます。
ファイアウォール ポリシーは、検査モード = プロキシ ベースで構成されており、Web フィルターが有効になっています。
FortiOS 7.6では、機能セット選択 (フローベースまたはプロキシベース) を持つセキュリティプロファイルは、ファイアウォールポリシーで使用されるインスペクションモードと一致する必要があります。プロファイルの機能セットがポリシーのインスペクションモードと一致しない場合、プロファイルの動作は管理者の期待と一致しません（多くの場合、FortiOSによって正しい使用/選択が妨げられたり、機能の動作が意図したとおりに適用されなかったりします）。
この不一致により、www.facebook.com に設定された URL フィルタ エントリ (監視に設定) が期待どおりの結果を生成せず、代わりにセッションがカテゴリ評価によって評価され、ブロックされる (FortiGuard

ブロック ページで悪意のある Web サイトとして表示される) 理由が説明されます。
他のオプションが最適ではない理由:
A: Web 評価のオーバーライドは展示物には表示されず、オーバーライドの構成ミスを示すものもありません。
C: ポリシー検査モードは変更できますが、表示される根本原因はプロファイル機能セットの不一致です (プロファイルはフローベースです)。
D: 表示される URL フィルター アクションはモニターであり、これだけではブロック ページは生成されません。

最新問題**: 64**
展示品を参照してください。

定義済みのディープ インスペクション プロファイルとカスタム ディープ インスペクション プロファイルでは、図 「これらの Web カテゴリが除外される 2 つの理由は何ですか (2 つ選択してください)」に示すように、一部の Web カテゴリが SSL インスペクションから除外されます。
A. これらの Web サイトは FortiGate の信頼できるドメイン リストに含まれているため、リソースの使用率が最適化されます。
B. 法的規制は、ユーザーのプライバシーを優先し、これらの Web サイトの機密情報を保護することを目的としています。
C. これらの Web サイトは、FortiGuard によって管理されている信頼できるドメイン名の許可リストに含まれています。
D. FortiGate の一時証明書は、HTTP Strict Transport Security を使用する Web サイトへのブラウザのアクセスを拒否します。
Answer: B,C (メーッセージを残す**)**
FortiOS 7.6では、定義済みのディープ・インスペクションおよびカスタム・ディープ・インスペクションSSLインスペクションプロファイルにおいて、特定のウェブカテゴリ（金融銀行、健康・ウェルネスなど）とよく知られたドメイン（Apple、Google、Adobeなど）が意図的に除外されます。この動作は文書化されており、意図的なものです。
正しい理由は 2 つあります。
B. 法的規制は、ユーザーのプライバシーを優先し、これらのウェブサイトの機密情報を保護することを目的としています。
正しい
金融と銀行、健康とウェルネスなどのカテゴリでは、通常、機密性の高い個人データが扱われます。
多くのプライバシーおよびコンプライアンス規制 (GDPR、PCI-DSS、HIPAA のような要件など) では、このようなトラフィックに対する SSL インターセプトを推奨または制限しています。
法的およびコンプライアンス上のリスクを軽減するために、FortiOS ではこれらのカテゴリをデフォルトで SSL ディープ インスペクションの対象から除外しています。
これは、FortiOS SSL/SSH 検査ドキュメントに明示的に記載されています。
C. これらのウェブサイトは、FortiGuard が管理する信頼できるドメイン名の許可リストに登録されています。
正しい
FortiGuard は、よく知られているサービスやプラットフォームの評判の高い/信頼できるドメイン リストを維持します。
これらのドメインは、次の理由でデフォルトでディープ インスペクションから除外されます。
アプリケーションの破損を防ぐ

証明書のピン留めと互換性の問題を回避する
ユーザーエクスペリエンスを維持する
このため、Apple、Google、Adobe、アプリストアなどのドメインは SSL 検査の例外として表示されます。
他の選択肢が間違っている理由
A. リソース利用の最適化
正しくない。
検査を減らすことでリソースを節約できますが、これがこれらのカテゴリを免除する主な理由として文書化されているわけではありません。
D. FortiGateの一時証明書がHSTSウェブサイトへのアクセスを拒否
正しくない。
HSTS と証明書ピンニングは SSL 検査で問題を引き起こす可能性がありますが、このオプションは副作用を説明するものであり、免除の理由を説明するものではありません。
この免除は、証明書がアクセスを拒否するためではなく、そのような問題を回避するために存在します。