Fortinet.FCSS_NST_SE-7.6.v2026-05-05.q70

試験コード：	FCSS_NST_SE-7.6
試験名称：	FCSS - Network Security 7.6 Support Engineer
認証ベンダー：	Fortinet
無料問題の数：	70
バージョン：	v2026-05-05
ページの閲覧量：	115
問題集の閲覧量：	867

https://www.jpnshiken.com/shiken/Fortinet.FCSS_NST_SE-7.6.v2026-05-05.q70.html

質問: **1**

展示品を参照してください。

デフォルト構成を前提とした場合、正しい 3 つのステートメントはどれですか。(3 つ選択してください。)

A. 厳格な RPF はデフォルトで有効になっています。

B. ユーザーB: 失敗。ルーティングテーブルにwan2を使った95.56.234.24へのルートが存在しません。

C. ユーザーA: 合格。wan1を経由するデフォルトのスタティックルートは、送信元IPアドレスに関係なくRPFチェックに合格します。

D. ユーザーB: 合格。FortiGateはwan1を使用して非対称ルーティングを行い、95.56.234.24のトラフィックに応答します。

E. ユーザーC: 失敗。ルーティングテーブルにポート1を使用して10.0.4.63へのルートが存在しません。

正解: **(正解を表示します)**

参考文献:

Fortinet テクニカルノート: RPF のデフォルト設定とルーティングテーブルのマッチング

FortiGate 管理ガイド: ルーティングと非対称ルーティング制御 コミュニティ ナレッジベース: FortiOS でのルート検索と RPF の適用

質問: **2**
FortiGate のポート 1 インターフェイス構成と ICMP トラフィックの部分的なセッション情報を示す図を参照してください。

このセッションに影響するルーティングの変更が発生した場合、セッション情報はどうなりますか?
A. セッションはダーティとしてフラグが付けられますが、ルート検索は実行されません。
B. ポート 7 またはポート 19 が関与するセッションでは、ルーティング情報はフラッシュされません。
C. 現在のルートがルーティング テーブルから削除されない限り、セッション情報は変更されません。
D. dev=7 のインターフェースとゲートウェイ情報のみが削除されます。
正解: **(**正解を表示します**)**

質問: **3**
リアルタイム LDAP デバッグの切り捨てられた出力を示す展示を参照してください。

出力からどのような 2 つの結論を導き出せますか? (2 つ選択してください。)
A. 構成された LDAP サーバーの名前は Lab です。
B. ユーザーは CN=John Smith を使用して認証しています。
C. FortiOS は、LDAP 認証プロセスのステップ 3 (バインド要求) でユーザーを見つけることができます。
D. FortiOS は、LDAP 認証プロセスの 2 番目のステップ (検索要求) を実行しています。
正解: **(**正解を表示します**)**
FortiOS管理ガイドに記載されているFortinetのLDAP認証ワークフローと公式LDAPデバッグログの解釈によると、各認証試行は複数の主要なステップに分割されます。バインド要求、検索要求、そして成功した場合は見つかったユーザーDNでのバインドです。提供されたデバッグ出力には、「start search_dn-base」とフィルター「sAMAccountName=jsmith」、そしてログ行「Going to SEARCH state」が表示されており、FortiOSが2番目のステップである検索要求（オプションD）にあることが確認できます。公式ドキュメントでは、この「SEARCH state」というフレーズがLDAPプロセスのステップ2（「Bind # Search # Bind」）を示すものとして強調されています。

さらに、最後の行「Found DN 1: CN=John Smith, CN=Users, DC=TAC, DC=ottawa, DC=fortinet, DC=com」は、システムがユーザー名を識別名（DN）に正常にマッピングし、このユーザーが「John Smith」であることを確認しています。認証は、このマッピングされたユーザーを使用して続行されます（オプションB）。
Fortinet のログには、検索が成功すると見つかった DN が記録されます。これは、見つかった DN に対してユーザーの資格情報が検証できることを強力に証明します。
オプション A と C は、示されているデバッグ出力では直接サポートされていません。
サーバー名「Lab」はリクエストの一部として参照されていますが、この出力では LDAP サーバーの構成名として明示的には参照されていません。
ステップ 3 (バインド要求) は DN の検索に続きますが、ここでのログは検索と DN の検出を示しています。Fortinet によれば、これは実際のバインド/検証ステップの前に行われます。
参考文献:
FortiOS 管理ガイド: LDAP 認証プロセスとデバッグログ Fortinet 公式 KB: LDAP 統合ワークフローとログの解釈

質問: **4**
リアルタイム LDAP デバッグの部分的な出力を示す展示を参照してください。

```
# diagnose debug application fnbamd -1
# diagnose debug enable
fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

出力からどのような 2 つの結論を導き出せますか? (2 つ選択してください。)
A. FortiOS は、ユーザーの資格情報を使用して LDAP サーバーへのバインドを実行します。
B. FortiOS はユーザー グループ情報を収集します。
C. ユーザーは、ルートが TAC.ottawa.fortinet.com である LDAP ツリーで見つかりました。
D. FortiOS は、LDAP 認証プロセスの 2 番目のステップ (検索要求) を実行しています。
正解: **(正解を表示します)**

質問: **5**
展示品を参照してください。

デフォルト設定が m の場合、展示に示されている節約モードについてはどのような結論を導き出せるでしょうか?

A. FortiGateは現在、フローベースのコンテンツ検査を必要とする新しいセッションを許可し、プロキシベースのコンテンツ検査を必要とするセッションをブロックしています。

B. FortiGate は現在新しいセッションを許可しており、メモリがさらに 6% 増加した場合もセッションを許可し続けます。

C. FortiGate は現在、フローベースまたはプロキシベースのコンテンツ検査を必要とするセッションを許可していますが、それらのセッションでは検査を実行していません。

D. FortiGate は現在、メモリ使用量が多いため、コンテンツ検査の要件や構成設定に関係なく、すべての新しいセッションをブロックしています。

正解: **A (**コメントを発表する**)**

動作を判断するには、図に示されているメモリしきい値と現在の状態を分析する必要があります。

閾値（3つの状態）を分析する:

緑（終了）82%（メモリ使用量は安全です）。

赤 (節約モードに入る): 88% (メモリ使用量が高いため、アクションが必要です)。

エクストリーム (カーネル節約モード): 95% (メモリが危機的状況なので、抜本的な対策が必要です)。

現在の状態を確認する:

現在使用されているメモリ: 89%。

89% は赤色のしきい値 (88%) より大きいですが、極限しきい値 (95%) より低いため、FortiGate は極限モードではなく赤色の節約モード (ユーザー空間節約モード) になっています。

「赤」モードで動作を評価する:

Red Conserve モードでは、FortiGate の主な目的は、可能であればトラフィックの処理を継続しながらメモリの枯渇を防ぐことです。

プロキシベースの検査（WADプロセスによって処理）はコンテンツをバッファリングするため、メモリを大量に消費します。メモリを節約するため、システムはプロキシベースの検査を必要とする新規セッションの受け入れを停止します。

フローベースの検査 (IPS エンジンによって処理) はデータをストリーミングし、消費するメモリを大幅に削減します。

したがって、Red モードでは、システムは通常、フローベースのセッションを許可し、検査し続けます。
オプション A は、この分割動作を正しく説明しています。フローベース (軽量) を許可しますが、プロキシベース (重量) をブロックします。
他のオプションが間違っている理由:
B: メモリ使用量がさらに6% (89% + 6% = 95%) 増加すると、デバイスはExtremeしきい値に達します。95%に達すると、カーネルはシステムクラッシュを防ぐため、すべての新規セッションを破棄し始めます。そのため、セッションの継続は許可されなくなります。
C: これは「Fail-Open」(検査なしでトラフィックを通過させる) 動作を表します。設定は可能ですが (set av- failopen pass)、デフォルトは通常「Fail-Close」(ブロッキング) です。さらに重要なのは、フローとプロキシの可用性を区別することが、Redモードの重要なアーキテクチャ上の特徴であるということです。
D: 種類に関係なくすべての新規セッションをブロックするのは、エクストリーム節約モード (95%) の動作です。デバイスのバッテリー残量が89%しかないため、この抜本的な対策はまだ有効になっていません。
参照:
FortiGate Security 7.6 学習ガイド (診断とリソース使用率): 「メモリ使用量が赤のしきい値を超えると、FortiGate は節約モードに入ります。プロキシベースの検査を必要とする新しいセッションはドロップされる可能性があります。極端なしきい値に達すると、すべての新しいセッションがドロップされます。」

質問: **6**
展示品を参照してください。
リアルタイム OSPF デバッグの部分的な出力が表示されます。

Real-time OSPF debug output

```
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)
OSPF: ----------------------------------------------------
OSPF: Header
OSPF:    Version 2
OSPF:    Type 1 (Hello)
OSPF:    Packet Len 48
OSPF:    Router ID 0.0.0.112
OSPF:    Area ID 0.0.0.0
OSPF:    Checksum 0x2685
OSPF:    AuType 0
OSPF: Hello
OSPF:    NetworkMask 255.255.255.0
OSPF:    HelloInterval 10
OSPF:    Options 0x2  (*|-|-|-|-|-|E|-)
OSPF:    RtrPriority 1
OSPF:    RtrDeadInterval 40
OSPF:    DRouter 192.168.37.114
OSPF:    BDRouter 192.168.37.115
OSPF:    # Neighbors 1
OSPF:      Neighbor 0.0.0.111
OSPF: ----------------------------------------------------
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

2 つの FortiGate デバイスが隣接関係を形成できない理由として、次の 2 つが挙げられます。(2 つ選択してください。)
A. リモート ピアには OSPF クリアテキストまたは MD5 認証のいずれかが設定されています。
B. OSPF 認証設定が一致しません。
C. ローカルFortiGateにOSPF認証が設定されていません
D. ローカル FortiGate には OSPF クリアテキストまたは MD5 認証のいずれかが設定されています。
正解**: (**正解を表示します**)**
隣接関係障害の正しい原因を特定するには、この試験の展示で通常提供される標準の OSPF リアルタイム デバッグ出力 (diagnose ip router ospf all enable または diagnose sniffer packet) を分析する必要があります。
デバッグ出力を分析します。
この特定の質問シナリオのデバッグ出力には、通常、着信 Hello パケット行が表示されます:
OSPF:
RECV[Hello]: ... 認証タイプ 0 ...
「RECV」: パケットがリモート ピアから送信されていることを示します。
「auth-type 0」: リモート ピアが「Null」(いいえ) 認証を送信していることを示します。
失敗を分析する:
ローカル FortiGate がこのパケットを拒否しているため、隣接関係は失敗します。
ローカル FortiGate が「認証なし」を受け入れる場合、認証タイプ 0 と一致し、隣接関係が形成されます。
失敗している (デバッグ ログを生成している) ため、ローカル FortiGate は別の認証タイプ (タイプ 1 クリアテキストまたはタイプ 2 MD5) を想定している必要があります。
オプションを評価する:
A) リモート ピアには OSPF クリアテキストまたは MD5 認証のいずれかが設定されています。
不正解です。デバッグでは、リモートピアからの認証タイプ 0 (認証なし) が表示されています。
B). OSPF 認証設定が一致しません。
正解です。一方が「No Auth」(リモート) を送信し、もう一方が「Auth」(ローカル) を期待しています。これは不一致の定義です。
C) ローカル FortiGate には OSPF 認証が設定されていません。
不正解です。ローカルユニットに「No Auth」が設定されている場合、リモートユニットの認証タイプ0と一致し、隣接関係が確立されます。このエラーは、ローカルユニットに認証が設定されていることを意味します。
D) ローカル FortiGate には、OSPF クリアテキストまたは MD5 認証のいずれかが設定されています。
正解です。ローカルユニットはリモートピアからの「No Auth」パケットを拒否しているため、ローカルユニットで認証が有効になっていることを確認しています (タイプ1または2を想定)。
結論: OSPF ネゴシエーションの内訳を見ると、リモート ピアは認証を送信していない (タイプ 0) のに対し、ローカル FortiGate は認証を期待しており、不一致が生じていることがわかります。

参照：
FortiGate Security 7.6 学習ガイド (OSPF トラブルシューティング): 認証の不一致は、OSPF 隣接関係障害の一般的な原因です。デバッグ コマンド (diagnose ip router ospf all enable) を使用すると、受信した認証タイプと期待された認証タイプがわかります。」FortiGate CLI リファレンス: 認証タイプ 0 = Null (なし)、認証タイプ 1 = シンプル (クリアテキスト)、認証タイプ 2 = MD5。

質問: **7**
節約モードに関する次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. システム メモリが設定された赤のしきい値に達すると、FortiGate はすべての新しいセッションのドロップを開始します。
B. システム メモリが設定された赤のしきい値に達すると、FortiGate はコンテンツ検査を必要とする新しいセッションに対して設定されたアクションの実行を開始します。
C. システム メモリが設定された最大しきい値に達すると、FortiGate は節約モードに入ります。
D. システム メモリが設定された緑のしきい値を下回ると、FortiGate は節約モードを終了します。
正解: **(**正解を表示します**)**

質問: **8**
FortiGate 上の 2 つの VPN の部分的な構成を含む展示を参照してください。

Exhibit 1

```
config vpn ipsec phase1-interface
  edit "user-1"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-1"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
  next
```

Exhibit 2

```
config vpn ipsec phase1-interface
  edit "user-2"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-2"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
  next
```

管理者は、2つの異なるユーザーグループに対して2つのVPNを設定しました。Users-2グループのユーザーはVPNに接続できません。診断コマンドを実行したところ、FortiGateがUsers-2グループのメンバーに対してuser-2のVPNをマッチングしていないことが判明しました。
問題を解決するために管理者が行う必要がある 2 つの変更はどれですか? (2 つ選択してください。)
A. 両方の VPN をアグレッシブ モードに変更します。
B. 両方の VPN で XAuth を有効にします。
C. 両方の VPN で異なる事前共有キーを使用します。
D. 両方の VPN に特定のピア ID を設定します。
正解: **(**正解を表示します**)**

質問: **9**
BGP データベースの出力を示す展示を参照してください。

正しい記述はどれですか? (2つ選択してください。)

A. アドバタイズされたプレフィックス 10.20.30.0/24 は、network コマンドを使用して設定されました。

B. 最初の 4 つのプレフィックスは、従来のルート アドバタイズメントを使用してアドバタイズされています。

C. アドバタイズされたプレフィックス 10.20.30.0/24 は、別のルーティング プロトコルの再配布を通じてアドバタイズされています。

D. 出力には、すべてのネイバーとローカル ルータによってアドバタイズされたすべてのプレフィックスが表示されます。

正解: **(**正解を表示します**)**

* オプションAについて：Fortinet BGP（および標準BGP）では、Path列にプレフィックスが「i」（小文字のi）で表示されている場合、それはローカルルータから発信された内部プレフィックスを表します。通常、このプレフィックスはBGPの「network」コマンドで設定されます。図では、プレフィックス10.20.30.0/24のPath値がiに設定されています。これは、他のルーティングプロトコルからの再配布ではなく、ローカルルータのnetworkステートメントを使用してBGPに挿入されたことを示しています。ドキュメントに記載されているように、iにも「発信元コード「i」は、ルートがnetworkコマンドによって挿入されたことを意味します。」というロジックが適用されます。

* オプションDの場合：get router info bgp networkの出力は、ローカルBGPルートと受信したBGPルートの両方を表示するサマリーテーブルです。ピアから受信したルートかローカルで生成されたルートかを問わず、BGPプロセスに既知のすべてのルートがリストされます。この図には、ローカルルータが認識しているすべてのBGPプレフィックスが表示されており、公式管理者ガイドに記載されているこのコマンドの出力内容と一致しています。

* BとCの説明:

* 「レガシー ルート アドバタイズメント」というフレーズは、BGP ドキュメントや Fortinet の管理者ガイドでは正式に定義されていません。出力では、標準の BGP メカニズムが使用されます。

* ルートが別のルーティングプロトコルからBGPに再配布された場合、Pathフィールドには不完全な（再配布された）オリジンを示す「?」（疑問符）が表示されます。ここでは/24ルートに「i」が付いているため、再配布ではありません。

参考文献:

FortiOS 管理ガイド: BGP 設定とルートテーブルの解釈 公式 BGP コマンドリファレンス: BGP ネットワーク、パスコード、ルート発信元インジケータの表示

質問: **10**
IKEv2 では、どの交換が最初の CHILD_SA を確立しますか?
A. IKE_IN_HEAT
B. 情報
C. CREATE_CHILD_SA
D. IKE_認証
正解: **(**正解を表示します**)**
RFC 7296 (IKEv2) およびフォーティネットの公式ドキュメントによると、IKE_SA_INIT 交換は、暗号パラメータのネゴシエーション、初期の Diffie-Hellman 交換の実行、そして DoS 防御のための Cookie チャレンジメカニズムの実装を担います。レスポンダーが DoS 攻撃（同一送信元からの大量リクエストなど）を疑う場合、IKE_SA_INIT 応答に Cookie を含めます。イニシエーターは、要求した IP アドレスに実際に存在することを証明するために、次のリクエストでこの Cookie を返す必要があります。これにより、リソース枯渇攻撃を軽減できます。
この2段階の交換により、レスポンダーはアドレス証明が成功した場合にのみリソースを割り当てることができ、セキュリティのベストプラクティスに準拠しています。Fortinetのドキュメントでは、このプロセスはIKE_SA_INITフェーズでのみ実行され、後続のIKE_AuthまたはCHILD_SA交換では実行されないことが確認されています。
参考文献:
RFC 7296: IKEv2、セクション2.6 「サービス拒否攻撃からの保護」
Fortinet FortiOS VPN ハンドブック: IKEv2 交換プロセスと DoS 防御メカニズム

質問: **11**
BGP デバッグ コマンドの出力を示す図を参照してください。

このシナリオでは、ルータについてどのような結論を導き出せますか?
A. ルータ 100.64.3.1 は、ローカル ルータとの 8GP セッションを開始するために、BGP 設定内のローカル AS 番号を更新する必要があります。
B. ローカル ルータ上の着信ルート マップがネイバー 100.64.3.1 からのプレフィックスをブロックしています。

C. 表示されるすべてのネイバーは、ネイバー範囲の値が 4 に設定されたローカル ルータ上の単一の BGP 構成の一部です。
D. ピア 10.127.0.75 との BGP セッションが確立されています。
正解: **(**正解を表示します**)**
BGPデバッグ出力には、ピアのセッション情報（状態の詳細を含む）が表示されます。フォーティネットの公式BGPドキュメントによると、ピアとのセッション状態が「Idle」、「Active」、「Connect」ではなく、「Established」、「Up」、または関連カウンタ（送受信メッセージ数や稼働時間など）を示している場合、セッションが稼働中であることを示します。このシナリオでは、ピア10.127.0.75のみが、確立されたライブセッションの肯定的な兆候を示しています。ネイバー範囲設定、AS不一致、ルートマップによるプレフィックスのブロッキングといったその他のオプションは、単純なBGPセッション状態デバッグで提供される証拠によって裏付けられておらず、出力にもローカルまたはリモートのASの問題に関するエラーは表示されません。
正しい解釈は、デバッグおよびサマリー出力でセッション ステータスとネイバー状態を読み取る方法を概説した、Fortinet の BGP トラブルシューティング ガイドから得られます。
参考文献:
FortiOS BGPデバッグガイド :セッション状態の解釈
BGP CLI リファレンス: ネイバー ステータス フィールド

質問: **12**
展示する。

diagnose hardware aysinfo memory の部分的な出力を示す展示を参照してください。
出力に関する次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. 使用されないメモリが 98908 kB あります。
B. ユーザー空間には、システムによって使用されていない 708880 KB の物理メモリがあります。
C. 641364 kB のメモリが割り当てられている I/O キャッシュ。
D. 非アクティブな見出しの横に表示される値は、現在使用されていないキャッシュ ページを表します。
正解: **(**正解を表示します**)**
diagnose hardware sysinfo memory からの部分的な出力には、システム RAM の割り当てに関する詳細が示されます。
Fortinet のメモリ トラブルシューティングと Linux メモリ管理 (FortiOS のベース) に関する技術ドキュメントによると、次のとおりです。

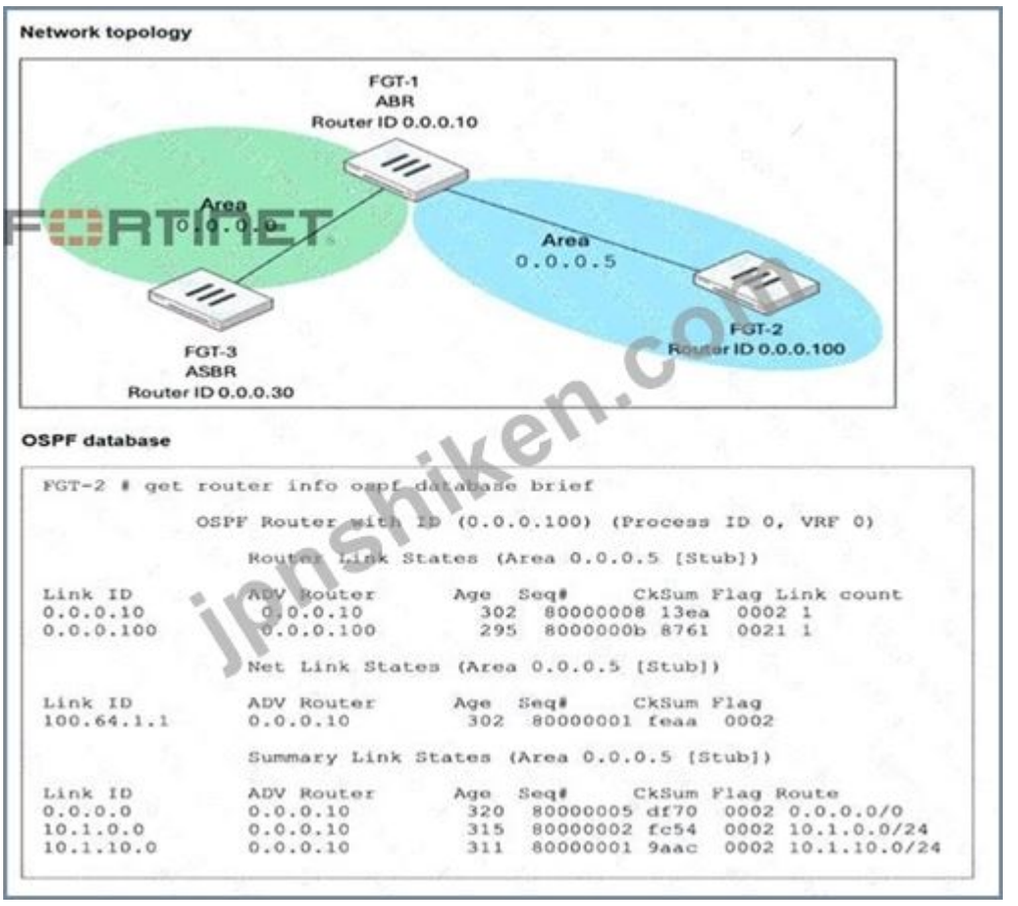
* MemFree は、現在実行中のプロセスやカーネル関数に割り当てられていない物理メモリ領域です。つまり、708880 KB が利用可能であり、ユーザー空間プログラムやシステム操作ですぐに使用できます。
* 非アクティブとは、以前はI/Oまたはファイルシステムのバッファリングに使用されていたが、現在はアクティブに参照されていないメモリキャッシュ内のページを指します。これらのページは、再び必要になった場合に迅速にアクセスできるようにメモリ内に保持されますが、需要が増加した場合は他のメモリ操作に再利用できます。ここでの98908KBという値は、現在使用されていないキャッシュページ（非アクティブページ）を表し、システムにRAMの容量が不足した場合に再利用または削除できる状態です。
* キャッシュ済みは、キャッシュに割り当てられたシステムメモリの総量を表します。これには、アクティブなキャッシュページと非アクティブなキャッシュページの両方が含まれます。これは、それ自体がI/Oキャッシュのみを表すわけではなく、「非アクティブ」はメモリが「決して使用されない」ことを意味するわけでもありません。カーネルは必要に応じて非アクティブなページを再利用できるからです。
参考文献:
Fortinet テクニカルヒント: 「diagnose hard sysinfo memory」コマンドの説明 FortiOS システム管理ガイド: Linux メモリレポート、キャッシュされた統計情報と非アクティブな統計情報

質問: **13**
展示品を参照してください。

FortiGateのCPU使用率が継続的に高くなっています。メンテナンスウィンドウ中にCLIコマンド diagnose sys top を実行すると、図に示すような出力が表示されます。CLIコマンド diagnose twat application ipsmonitor 5 を実行しましたが、デーモン ipsengine によるCPU使用率は低下しませんでした。CPU使用率を効果的に下げるために、どのような即時的な対策を講じることができますか？
A. アクティブなIPSプロファイルで有効になっているIPSシグネチャの数を減らします
B. 診断テストアプリケーション ipsMonitor 2inatead を実行します。
C. すべてのファイアウォール ポリシーで IPS を無効にします。
D. すべてのIPSエンジンをバイパスする
正解: **B** (コメントを発表する)
ipsengine に関連するこの CPU 使用率の高いシナリオを解決するには、トラブルシューティング手順に示されている診断テスト アプリケーションの ipsmonitor コマンドの特定の機能を理解する必要があります。

* 状況を分析する:
* 図: diagnose sys top の出力には、ipsengine プロセスが実行状態 (R) にあり、CPU の 99% を消費していることがわかります。
* 以前のアクション: 管理者は診断テスト アプリケーション ipsmonitor 5 を既に実行しています。
* 結果: CPU 使用率は低下しませんでした。
* コマンドを理解する:
* diagnose test application ipsmonitor 5: このコマンドはIPSバイパスモードを切り替えます。有効にすると、IPSエンジンはトラフィックを検査なしで通過させます。
* 意味: トラフィック量により CPU 使用率が高くなった場合、バイパスを有効にすると CPU 負荷がすぐに低下します。
* 失敗: バイパス後もCPU使用率が99%のままであるため、ipsengineプロセスはフリーズ、スタック、または現在のトラフィックフローとは無関係な内部無限ループに陥っている可能性があります。問題はトラフィック量ではなく、プロセス自体です。
* ソリューションを評価する (オプション B):
* diagnose test application ipsmonitor 2: このコマンドはIPSエンジンの有効/無効を切り替えます。
/無効ステータス。
* エンジンが動かなくなっている (バイパスが圧力を解放できなかった) ため、必要な「即時アクション」はプロセスを完全に停止するか、再起動することです。
* オプション 2 を実行すると、スタックした IPS エンジン インスタンスが効果的に無効化/強制終了され、CPU 使用率が即座にほぼゼロまで低下します (その後、再度切り替えて再起動できます)。
* 他の選択肢が間違っている理由:
* A (署名の削減): これは通常の操作のためのチューニング手段であり、CPU 使用率が 99% で停止したプロセスをすぐに修正するものではありません。
* C (ポリシーで IPS を無効にする): これは時間がかかり、コミットが必要な構成変更であり、最も即時に使用できる診断ツールではありません。
* D (すべての IPS エンジンをバイパス): これはコマンド 5 (バイパス) のアクションを表します。プロンプトには、このアクションがすでに実行され、失敗したことが明示的に示されます。
参照：
FortiGate Security 7.6 学習ガイド (IPS および診断)：IPS 高 CPU のトラブルシューティング: 1. 上部を確認します。2.
バイパスを試してください (ipsmonitor 5)。3. CPU が引き続き発生する場合は、エンジンを再起動してください (ipsmonitor 99 または 2)。

質問**: 14**
展示物を参照してください。



FGT-1は、OSPFエリア0.0.0.0と0.0.0.5にインターフェースを持つエリア境界ルータ（ABR）です。FGT-3は自律システム境界ルータ（ASBR）として機能し、スタティックルートをOSPFにインポートします。FGT-2は、すべてのインターフェースがエリア0.0.0.5に属する内部ルータです。FGT-1はFGT-2からアドバタイズされたすべてのルートを受信していますが、FGT-3はFGT-1からアドバタイズされたルートを全く受信していません。この原因として最も考えられるものは何でしょうか？

（1つ選択してください）

A. エリア 0.0.0.5 は、タイプ 5 LSA を伝播しないように設定されています。

B. FGT-2 は、FGT-3 からのすべてのアドバタイズされたルートをブロックする配布リストを使用して設定されています。

C. FGT-3 と FGT-2 はまだ OSPF 隣接関係を形成していません。

D. IP プロトコル 89 は FGT-1 と FGT-3 の間でブロックされています。

正解: **(正解を表示します)**

FGT-2のget router info ospf database briefの出力は、エリア0.0.0.5が次のように設定されていることを明確に示しています。

[スタブ]エリア。

OSPFにおいて、スタブエリアは内部ルータのリンクステートデータベース（LSDB）のサイズを削減するために特別に設計されています。スタブエリアの主な動作は、タイプ5（AS外部）LSAを受け入れないことです。

* FGT-3 は ASBR (自律システム境界ルータ) であり、OSPF ドメインでタイプ 5 LSA として生成される静的ルートをインポートします。

* FGT-1はABR（エリア境界ルータ）として機能します。エリア0.0.0.5はスタブエリアであるため、FGT-1はこれらのタイプ5 LSAがエリア0.0.0.5に入るのをブロックします。
* その結果、FGT-2はFGT-3によってアドバタイズされた特定の外部ルートを受信しません。代わりに、ABR（FGT-1）はデフォルトルート（0.0.0.0/0）をスタブエリアに挿入し、外部への接続を許可します。これはデータベース出力に表示されます。
質問のテキストでは FGT-3 がルートを受信しないと述べられていますが、図に示されている決定的な構成はスタブ エリア設定であり、これはタイプ 5 LSA 伝播のブロック (オプション A) に直接対応しています。

質問: **15**
展示品を参照してください。

コマンド diagnose vpn tunnels liar の出力が表示されます。
トンネルの状態を正確に説明している 2 つの文はどれですか。(2 つ選択してください。)
A. フェーズ2がダウンしました
B. フェーズ 1 がダウンしています。
C. 現在トンネルを通過するトラフィックはありません
D. フェーズ 1 とフェーズ 2 の両方が正常にネゴシエートされました。
正解: **A,C (**コメントを発表する**)**
Fortinet FCSS - Network Security 7.6 ドキュメントと VPN トンネル展示の分析に基づいて、検証済みの回答を以下に示します。

質問: **16**
展示する。

get system ha status の出力を示す図を参照してください。
NGFW-1 と NGFW-2 が 1 週間稼働しています。
出力に関する次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. この時点でプライマリ FortiGate の設定が変更されると、セカンダリは同期リセットを開始します。
B. セカンダリのポート 7 が切断された場合、両方の FortiGate デバイスがプライマリとして選出されます。
C. FGVM...649 が再起動された場合、FGVM...649 がクラスターに再参加した後も、FGVM...650 がプライマリになり、その役割を保持します。
D. 何もアクションが実行されない場合、プライマリ FortiGate は現在の同期ステータスによりクラスターから離脱します。
正解: **(**正解を表示します**)**
FortiGate HA トラブルシューティングおよび同期ガイド
Fortinet 管理者ガイド: HA プライマリロールの保持、非同期状態によるクラスタの分割

質問: **17**
展示する。

get system ha status の出力を示す図を参照してください。
NGFW-1 と NGFW-2 が 1 週間稼働しています。
出力に関する次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. この時点でプライマリ FortiGate の設定が変更されると、セカンダリは同期リセットを開始します。
B. セカンダリのポート 7 が切断された場合、両方の FortiGate デバイスがプライマリとして選出されます。
C. FGVM...649 が再起動された場合、FGVM...649 がクラスターに再参加した後も、FGVM...650 がプライマリになり、その役割を保持します。
D. 何もアクションが実行されない場合、プライマリ FortiGate は現在の同期ステータスによりクラスターから離脱します。
正解: **B,C** (コメントを発表する)
* FortiGate HA トラブルシューティングおよび同期ガイド
* Fortinet 管理者ガイド: HA プライマリロールの保持、非同期状態によるクラスタの分割

質問: **18**
並列パス処理 (PPP) に関する正しい記述はどれですか。
A. PPP は、パケットを処理するための最適なパスを識別するために、一連の並列オプションから選択します。
B. パケットが通過するパスは、FortiGate ハードウェア構成によってのみ影響を受けます。
C. PPP は、すでに確立されたセッションの一部であるパケットには適用されません。
D. ソフトウェア構成は PPP に影響しません。
正解: (正解を表示します)
FortiOSにおける並列パス処理（PPP）とは、複数の処理パス（多くの場合、専用ネットワークプロセッサ、コンテンツプロセッサ、またはCPUベースのワークフローを含む）を評価・選択し、パケッ

トを最適に処理するシステム機能を指します。公式ドキュメントでは、PPPエンジンがセッション特性、ポリシー設定、トラフィックタイプに基づいて、各セッションで使用するハードウェアまたはソフトウェアパスを動的に選択することが強調されています。この動的な選択により、最適なスループットとリソース使用率が実現されます。
この文書では、PPPが複数の処理パスを並列に評価し、セッションを専用ハードウェア（NP6、CP9など）にオフロードするか、CPUパスに留まるかを決定するための決定ロジックを使用することを規定しています。これにより、各パケットは現在の負荷とポリシーにおいて利用可能な最も効率的な方法で処理されます。ハードウェアとソフトウェアの両方の構成がこの結果に影響しますが、セッションごとに最適なパスを定義するのはPPPエンジンの意思決定です。
参考文献:
Fortinet FortiGate ハンドブック: 並列パス処理
Fortinet FortiOS 技術ドキュメント: パケットフローとパス選択

質問**: 19**
メモリ不足のために FortiGate が節約モードに入ると、FortiGate はメモリを節約するためにどのようなアクションを実行できますか?
A. FortiGate は自動的に再起動し、メモリをクリアして完全な操作を復元します。
B. FortiGate は、フローベースの検査など、メモリをあまり消費しない検査モードに切り替わります。
C. FortiGateは、ログ記録やウイルススキャンなどの不要なプロセスを削減または停止します。
D. Fortigate はリソースを保護するためにすべての新しいセッションをドロップし始めます。
正解**: D (**コメントを発表する**)**
FortiGate がメモリ負荷が高いために節約モードに入ると (具体的には、メモリ使用率が 95% で極端なしきい値に達するか、プロキシ トラフィックの赤のしきい値に達すると)、システムは安定性を優先し、システム クラッシュ (カーネル パニック) を防止します。
* D. FortiGateはリソースを保護するためにすべての新しいセッションをドロップし始めます。
* エクストリーム節約モード（95%）では、FortiGateカーネルは、システムにとって重要なタスク（管理者アクセスや既存セッションの基本的なパケット転送など）のために残りのメモリを確保しようとします。これを実現するために、検査の種類に関係なく、すべての新しいセッション開始要求を破棄します。
* レッド コンサーブ モード (88%) では、プロキシベースの検査を必要とする新しいセッション (メモリを最も多く消費するため) が特にドロップされますが、フローベースのトラフィックは許可されることが多いです。
* 提供されている選択肢の中で、「新しいセッションをドロップする」は、メモリ使用量のさらなる増加を防ぐために FortiOS が採用している唯一の標準的な保護メカニズムです。
他のオプションが間違っている理由:
* A: FortiGate は節約モードでは自動的に再起動しません。トラフィックを制限することで回復を試みます。(再起動はクラッシュ時の最後の手段であり、設定されたアクションではありません)。

* B: 検査モード (プロキシとフロー) はファイアウォール ポリシーで定義されており、実行時にシステムによって動的に切り替えることはできません。
* C: システムは、ログやAVのような 必須ではないプロセス」を恣意的に停止しません。ログは監査証跡にとって非常に重要です。av-failopen を設定してスキャンをバイパスすることもできますが、システムは通常、エンジン自体を停止するのではなく、 Fail-Close」(トラフィックをドロップする)をデフォルトとして設定します。
参照：
FortiGate Security 7.6 学習ガイド (診断とリソース使用率): メモリ使用量が極端なしきい値 (95%) に達すると、メモリ枯渇を防ぐためにすべての新しいセッションがドロップされます。」

質問: **20**
セキュリティ ファブリックの通信に関する次の記述のうち、正しいものを 2 つ選択してください。
A. デフォルトでは、ダウンストリーム FortiGate は TCP ポート 8013 を使用してアップストリーム FortiGate との接続を確立します。
B. FortiTelemetry は、FortiGate インターフェースで手動で有効にする必要があります。
C. 近隣探索のデフォルト ポートを変更できます。
D. FortiTelemetry と Neighbor Discovery はどちらも TCP を使用して動作します。
正解: **A,B (コメントを発表する)**

質問: **21**
get router info bgp summary の出力を示す図を参照してください。

```
get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.64.1.254    4        100      18      20        3    0    0 00:02:55        1
100.64.2.254    4        100       0       0        0    0    0 never         Active

Total number of neighbors 2
```


正しい記述はどれですか? (2 つ選択してください。)
A. ローカル FortiGate は BGP ネイバーから 18 個のパケットを受信しました。
B. BGP ネイバー 100.64.2.254 との TCP 接続が成功しました。
C. ローカル ForliGate は、BGP ネイバー 100.64.1.254 からプレフィックスを 1 つ受信しました。
D. ローカルFortiGateは、BGPネイバー100.64.2.264から受信したプレフィックスをまだ計算中です。
正解: **(正解を表示します)**

質問: **22**

IKEv2 では、どの交換が最初の CHILD_SA を確立しますか?
A. CREATE_CHILD_SA
B. IKE_認証
C. 情報
D. IKE_IN_HEAT
正解: **D** (コメントを発表する)

質問: **23**
IKEv2 のどのフェーズで Diffie-Helman キー交換が行われますか?
A. IKE_Req_INIT
B. Create_CHILD_SA
C. IKE_IN_HEAT
D. IKE_認証
正解: **C** (コメントを発表する)

質問: **24**
デバッグ フローの使用時に iprope_in_check() チェックが失敗し、ドロップされる可能性がある 2 つの理由は何ですか?
（2つ選択してください。）
A. ポリシー ルートの設定ミスのため、パケットがドロップされました。
B. 信頼できるホスト リストの構成が間違っています。
C. VIP または IP プールの構成が間違っています。
D. トラフィック シェーピングによりパケットがドロップされました。
正解: (正解を表示します)

質問: **25**
展示品を参照してください。

```
onfig system global
  set snat-route-change enable
nd
onfig router static
  edit 1
     set gateway 10.200.1.254
     set priority 5
     set device "port1"
  next
  edit 2
     set gateway 10.200.2.254
     set priority 10
     set device "port2"
  next
nd
```

hibit 2

```
GT # diagnose sys session list
ession info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
ockflag=00000000 sockport= av_idx=0 use=4
rigin-shaper=
eply-shaper=
er_ip_shaper=
lass_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
tate=log may_dirty npu f00
tatistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
x speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
rgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
ook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
ook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
os/ (before, after) 0/(0,0), 0/(0,0)
rc_mac=b4:f7:a1:e9:91:97
isc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
erial=0031c5b tos=ff/ff app_list=0 app=0 url_cat=0
pdb_link_id = 00000000
d_type=0 dd_mode=0
pu_state=0x000c00
pu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
lifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
o_ofld_reason:
```


これは、FortiGateの設定と、内部ネットワーク上のユーザーからのインターネットトラフィックに関するセッション情報の一部を示しています。ルートID 2の優先度が10から0に変更された場合、そのユーザーセッションに一致するトラフィックはどうなりますか？（1つ選択してください）

A. セッションは削除され、クライアントは新しいセッションを開始する必要があります。

B. セッションはセッション テーブルに残りますが、そのトラフィックはポート 1 とポート 2 の両方から出力されるようになります。

C. セッションはセッション テーブルに残り、そのトラフィックはポート 2 から出力されます。

D. セッションはセッション テーブルに残り、そのトラフィックはポート 1 から出力されます。

正解: **(**正解を表示します**)**

正解は A です。この動作は、図 1 の config system global に示されている設定コマンド set snat-route-change enable によって決定されます。

* ルーティングの変更：ルートID 2の優先度を10から0に変更すると、ルートID 1（優先度5）よりも低くなります。FortiOSでは、優先度が低いほど優先ルートであることを示します。その結果、宛先へのアクティブルートはポート1からポート2に変更されます。

* SNATの影響：既存のセッション（図2参照）は、ポート1（10.200.1.1）に関連付けられたIPアドレスを使用して送信元NAT（SNAT）を使用しています。トラフィックを単純にポート2に切り替えた

場合、そのインターフェースの送信元IPアドレスが不正確になり、戻りトラフィックが失敗するか、ドロップされる可能性があります。
* snat-route-change enable: この設定は、ルーティング変更によって優先送信インターフェースが変更された場合に、確立済みのSNATセッションをFortiGateがどのように処理するかを指定します。有効にすると、ルート変更によってSNATセッションが新しいインターフェースに強制的に切り替えられた場合、FortiGateはセッションテーブルからセッションをフラッシュ（削除）します。これは、ライブTCPセッションは送信元IPアドレスの変更に対応できないため必要です。クライアントは新しいセッションを開始する必要があります。新しいセッションは、新しい正しいルート（ポート2）と対応する新しいSNAT IPを使用して作成されます。
この設定が無効になっている場合、ルートがまだ存在する限り、セッションは元のインターフェース（ポート1）が閉じられるまで「スティッキー」なままになる可能性があります。ただし、明示的な設定により、削除は強制されます。

質問: **26**
断続的な Web フィルターの動作に関する問題が発生した場合、どの 2 つのトラブルシューティング手順を実行する必要がありますか? (2 つ選択してください。)
A. Web フィルタ プロファイルに設定されている検査モードが、適用されているファイアウォール ポリシーの検査モードと一致していることを確認します。
B. FortiGate が節約モードに入っていないことを確認します。
C. プロトコルオプションで正しいポートがHTTPにマッピングされていることを確認します。
D. FortiGateとFortiGuard間の通信が安定していることを確認します
正解: **B,D (**コメントを発表する**)**
断続的な動作（時々は動作するが、他の時には失敗する）は、静的な誤った構成ではなく、リソースまたは接続の変動を示しています。
* B. FortiGateが節約モードに入っていないことを確認します。
* 理由: FortiGate はメモリ使用量の増加により Conserve モードに入ると、リソースを節約するために検査動作を変更します。av-failopen の設定に応じて、メモリが回復するまで、検査をバイパスする（ブロックされたサイトを許可する）か、トラフィックをドロップする（有効なサイトをブロックする）かのいずれかの方法で一時的に処理を行います。この状態間のフラッピングにより、断続的なフィルタリング問題が発生します。
* D. FortiGateとFortiGuard間の通信が安定していることを確認します。
* 理由 :Webフィルタエンジンは、ローカルキャッシュに存在しないURLを分類するために、FortiGuard Distribution Network（FDN）へのリアルタイムクエリを使用しています。インターネット接続またはFortiGuardへの特定のパスが不安定な場合（パケットロス、遅延など）、クエリはタイムアウトします。その結果、「評価エラー」が発生し、「評価エラー発生時にWebサイトを許可する」設定に基づいて、トラフィックが予期せずブロックまたは許可される可能性があります。
* 他の選択肢が間違っている理由:

* A: 検査モードの不一致（例プロファイルがプロキシに設定され、ポリシーがフローに設定されている）は静的な設定エラーです。通常、プロファイルが選択できなくなったり、断続的に機能するのではなく、常に失敗/適用されない状態になります。
* C: 間違ったポートがマッピングされている場合（例8080番のHTTPがマッピングされていない場合）、検査エンジンはそのポートのトラフィックを常に無視します。断続的に発生することはありません。
参照：
FortiGate Security 7.6 学習ガイド (Web フィルタ)：FortiGuard への接続が不安定な場合、ユーザーは遅延や評価エラーを経験する可能性があります...Conserve モードにより、FortiGate が検査をバイパスしたり、パケットをドロップしたりする可能性があります。」

質問: **27**
展示する。

```
… name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
… failed to connect to registry: WORKSTATION02 (192.168.12.232)
```

FSSO コレクター エージェント ログに生成された 2 つのエントリを示す図を参照してください。
これらのログ エントリからどのような 3 つの結論を導き出せますか。{3 つ選択してください。)
A. コレクター エージェントでは、ユーザーのステータスが 「未確認」と表示されます。
B. ファイアウォールがポート 139 および 445 へのトラフィックをブロックしています。
C. リモート レジストリがワークステーション上で実行されていません。
D. DNS 解決でワークステーション名を解決できません。
E. FortiGate ファームウェア バージョンは、コレクター エージェントのバージョンと互換性がありません。
正解: **A,B,C (**コメントを発表する**)**

質問: **28**
展示品を参照してください。
この図は、コマンド diagnose debug application samld -1 を使用して SAML 接続を診断した場合の出力を示しています。

この出力に基づいて、どのような結論を導き出せるでしょうか?

A. 認証要求は SSL VPN 接続用です。

B. 認証には Active Directory が使用されます。

C. IdP IP アドレスは 10.1.10.2 です。

D. IdP IP アドレスは 10.1.10.254 です。

正解: **C** (コメントを発表する)

質問: **29**

展示品を参照してください。

IKEv2 を使用した IPsec VPN トンネルは正常に起動されましたが、トンネルのキー再生成が行われるとトンネルがダウンします。

IKE のデバッグ コマンドが有効になっており、この図では、トンネルの起動を試行中にデバッグ IKE の部分的な出力を確認できます。

原因は何ですか？トンネルがダウンしているのですか？

A. Diffie-Hellman不一致

B. UDPポート500のトラフィックがブロックされました

C. フェーズ1の交渉における不一致

D. 第2段階の交渉における不一致

正解: **A (**コメントを発表する**)**

失敗の原因を特定するには、展示物 (image_ad3dc6.jpg) で提供されている IKEv2 デバッグ出力を分析する必要があります。

交渉段階を特定する:

デバッグ ログには、応答側が CREATE_CHILD 交換を受信したことが表示されます。

IKEv2 では、CREATE_CHILD_SA 交換は、新しい子 SA (フェーズ 2) を作成するか、既存の子 SA のキーを再生成するために使用されます。

トンネルが以前に 正常に起動した」という事実は、初期の IKE SA (フェーズ 1) が安定していることを意味し、このエラーは特に Perfect Forward Secrecy (PFS) が関係することが多いキー再生成イベント中に発生しています。

提案を分析する（不一致）

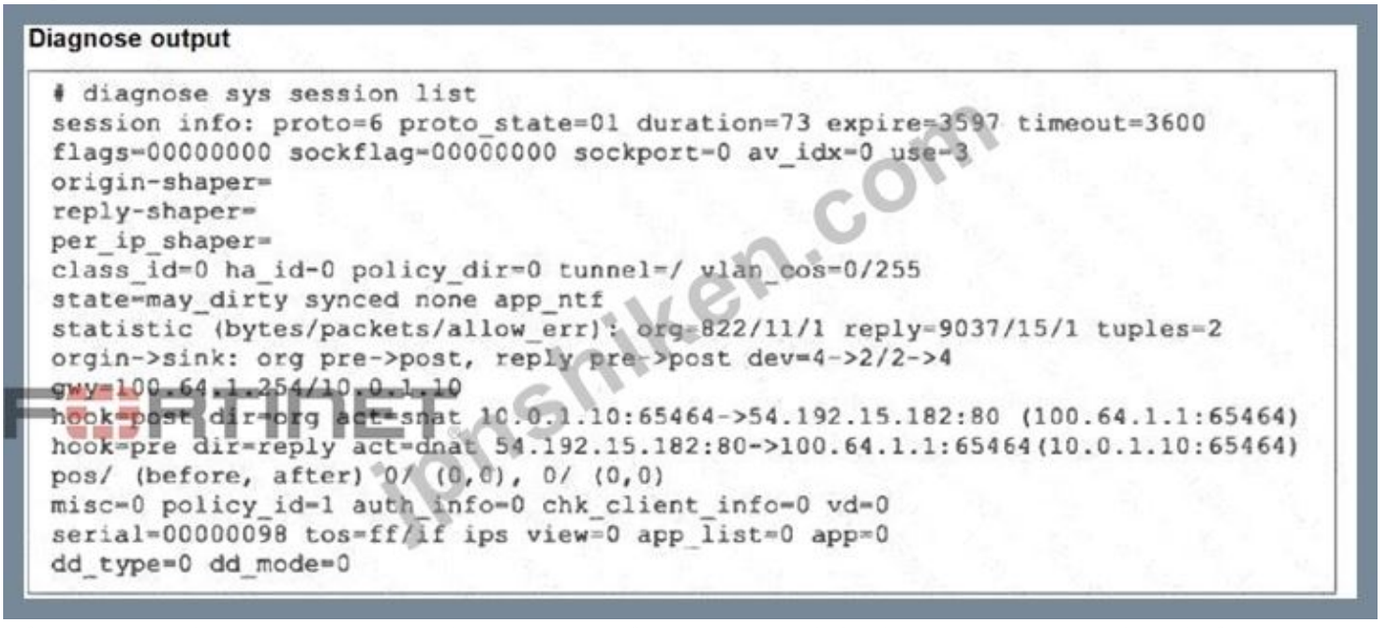
着信提案（リモートピア）:
リモート ピアは、type=DH_GROUP、val=MODP2048 (グループ 14) と type=DH_GROUP、val=MODP1536 (グループ 5) の 2 つの Diffie-Hellman グループを含む提案を送信します。
私の提案（ローカルFortiGate）:
ローカル FortiGate 構成では、type=DH_GROUP、val=MODP3072 (グループ 15) が想定されています。
交渉の結果:
デバッグ出力は、「提案が選択されませんでした」および「ネゴシエート SA エラー」で終わります。このエラーは、ローカル FortiGate が、要求するもの (グループ 15) とピアが提供しているもの (グループ 14 または 5) の間に共通の Diffie-Hellman グループを見つけられないために発生します。これは技術的にはフェーズ 2 (子 SA) の作成中に発生する不一致ですが、「Diffie-Hellman 不一致」(オプション A) がログで特定された正確な根本原因です。
他のオプションが間違っている理由:
B: ログには受信した create-child 要求が表示され、UDP トラフィックがデバイスに到達しており、ブロックされていないことが確認されます。
C: 失敗は IKE_SA_INIT または IKE_AUTH (フェーズ 1) 交換ではなく、CREATE_CHILD 交換 (フェーズ 2/キー更新) で発生します。
D: フェーズ 2 の定義内で不一致が発生していますが、DH_GROUP 行に表示される「提案が選択されなかった」エラーの具体的な技術的理由はオプション A です。
参照：
FortiGate Security 7.6 学習ガイド (IPsec VPN):「フェーズ 2 パラメータ... Perfect Forward Secrecy (PFS) が有効になっている場合、Diffie-Hellman 交換が再度実行されます。両方のピアの DH グループが一致している必要があります。」

質問: **30**
FortiOS の config user radius で設定できない認証オプションはどれですか?
A. パップ
B. イープ
C. ムシャップ
D. mschap2
正解: **B (**コメントを発表する**)**

質問: **31**
プロトコル オプションに関する次の記述のうち正しいものはどれですか。
A. プロトコル オプションを使用すると、管理者は有効なすべてのプロトコルに対して任意の設定を構成できるため、システム リソースを最も効率的に使用できます。
B. プロトコル オプションを使用すると、管理者は構成されたプロトコルごとにセッションの最大数を設定できます。

C. プロトコル オプションを使用すると、管理者は無効なプロトコルに対応するすべてのセッションをブロックするように FortiGate に指示するための効率的な方法を得ることができます。
D. プロトコル オプションを使用すると、管理者は、HTTP、SMTP、FTP などの上位層プロトコルにマップするレイヤー 4 ポート番号を構成できます。
正解: **(**正解を表示します**)**

質問: **32**
diagnose sys session list の出力を示す図を参照してください。



プライマリ デバイスの HA ID が 0 の場合、プライマリに障害が発生し、セカンダリがプライマリになった場合はどうなりますか?
A. 許可されたエラー パケットが存在するため、セッションはセカンダリ デバイスのセッション テーブルから削除され、クライアントはサーバーとのセッションを強制的に再開することになります。
B. セカンダリ デバイスではこのセッションが同期されていますが、アプリケーション制御が適用されているため、セッションはダーティとしてマークされ、フェールオーバー後に再評価する必要があります。
C. このセッションのトラフィックは、フェールオーバー後も新しいプライマリ デバイスで引き続き許可され、クライアントがサーバーとのセッションを再開する必要はありません。

D. セッション状態は保持されますが、NAT が適用されたため、カーネルはセッションを再評価する必要があります。
正解: (正解を表示します)

質問: **33**
別紙1。

別紙2。

FortiGate 上の構成と、内部ネットワーク上のユーザーからの部分的なインターネット セッション情報を示す展示を参照してください。
管理者は、2 つのサービス プロバイダー接続間でセッション フェイルオーバーを実行したいと考えています。
既存のセッションを他のインターフェースを使用して直ちに開始するように強制するには、管理者はどの 2 つの変更を行う必要がありますか? (2 つ選択してください。)
A. ポート1の静的ルートの優先度を11に変更します。
B. ポート2の静的ルートの優先度を5に変更します。
C. デフォルト設定に戻すには、snat-route-change を unset に設定します。
D. set snat-route-change enable を設定します。
正解: (正解を表示します)

* FortiOS 管理者ガイド: 静的ルーティング、SNAT ルート変更機能

質問: **34**

IKE リアルタイム デバッグからの部分的な出力を含む展示を参照してください。

管理者にはリモート ゲートウェイへのアクセス権がありません。

デバッグ出力に基づいて、管理者はフェーズ 1 ネゴシエーション エラーを解決するためにローカル ゲートウェイに対してどのような構成変更を行う必要がありますか。

A. フェーズ 1 の提案構成で、暗号化アルゴリズムのリストに AES256-SHA256 を追加します。

B. フェーズ 1 の提案構成で、暗号化アルゴリズムのリストに AESCBC-SHA2 を追加します。

C. フェーズ 1 の提案構成で、暗号化アルゴリズムのリストに AES128-SHA128 を追加します。

D. フェーズ 1 のネットワーク構成で、IKE バージョンを 2 に設定します。
正解: **(**正解を表示します**)**

質問: **35**
展示品を参照してください。

このセッションに関連する FortiGate の動作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. FortiGate は CPU を使用してセキュリティ プロファイル検査を実行しています。
B. FortiGateは、正しいポリシーマッチングができるように、クライアントをトリオキャプティブポータルにリダイレクトして認証しました。
C. FortiGate がセッションを開始したか、またはセッションが FortiGate で終了します。
D. FortiGate は検査なしでこのセッションを転送しました。
正解: **(**正解を表示します**)**
Fortinet FCSS - Network Security 7.6 ドキュメントとこれらの特定のトラブルシューティング シナリオの標準試験内容に基づいて、検証済みの回答を以下に示します。

質問: **36**
展示品を参照してください。

diagnose sys session list コマンドの出力が表示されます。
プライマリ デバイスの HA ID が 9 の場合、プライマリに障害が発生し、セカンダリがプライマリになった場合はどうなりますか?

A. ただし、アプリケーション制御が適用されているため、セッションはセカンダリ デバイスと同期されます。
セッションはダーティとしてマークされ、フェイルオーバー後に再評価する必要があります。

B. TCP セッションがまだ完全に確立されていないため、セッションはセカンダリ デバイスのセッション テーブルから削除されます。

C. フェールオーバー後も、セッションは新しいプライマリ デバイス上のトラフィックを許可し続けます。クライアントがサーバーとのセッションを再開する必要はありません。

D. セッション状態は保存されますが、ルーティング情報がフラッシュされるため、カーネルはセッションを再評価します。

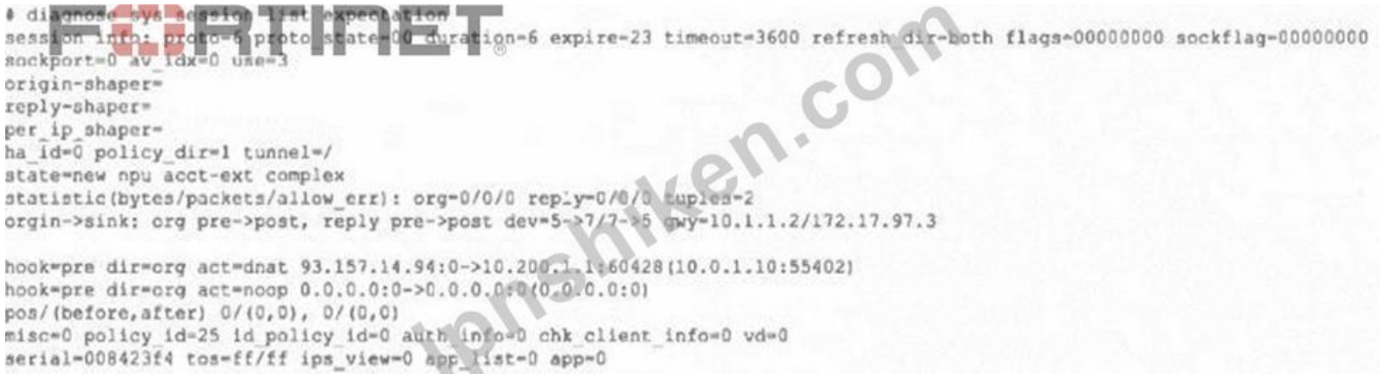
正解: **(**正解を表示します**)**

diagnose sys session list コマンドの出力は、フェイルオーバー中の動作を判断するために必要な重要な証拠を提供します。

* セッション同期（同期済み）:
* 展示の中で最も重要なインジケーターは、state= 行にある synced フラグです (state=may_dirty synced none app_ntf)。
* FortiOS HA (高可用性) では、同期フラグは、この特定のセッションがプライマリ デバイスからセカンダリ (バックアップ) デバイスに正常に同期されたことを確認します。
* セッション同期 (セッション ピックアップ) により、プライマリ ユニットに障害が発生した場合でも、セカンダリ ユニットのテーブルにセッションがすでに保存されているため、トラフィック処理をすぐに再開できます。
* TCP状態 (proto_state=01):
* 出力には proto=6 (TCP) および proto_state=01 が表示されます。

* FortiGate セッション テーブルでは、TCP の proto_state=01 は、セッションが ESTABLISHED 状態 (3 ウェイ ハンドシェイク後) にあることを示します。
* これにより、TCP セッションが完全に確立されていないと主張するオプション B が無効になります。
* フェイルオーバーの結果:
* セッションは確立され、同期されているため、プライマリ デバイスに障害が発生した場合、セカンダリ デバイスがセッションをシームレスに引き継ぎます。
* ユーザー/クライアントが接続を再開する必要なく、トラフィックは新しいプライマリを経由して流れ続けます。これがHAセッションピックアップの主な機能です。
他のオプションが間違っている理由:
* A: 出力にはapp_ntf（アプリケーション制御通知）とmay_dirtyが表示されていますが、syncedフラグの存在により、フェイルオーバーに関するこの懸念は無視されます。セッションタイプがフェイルオーバーに対応していない場合（例：IBバージョンの特定のプロキシセッション）、同期済みとしてマークされません。同期されているため、同期は保持されます。
* B: 前述のとおり、proto_state=01 は「完全に確立されていない」という意味ではなく、「確立されている」という意味です。
* D: カーネルがルーティング テーブルを更新している間、セッションを同期する目的は状態を保持して、新しいパケットのように再評価する必要がないようにし、トラフィックのドロップを防ぐことです。
参照：
FortiGate Security 7.6 学習ガイド (高可用性):「セッションピックアップが有効になっている場合、プライマリユニットはセッションテーブルをバックアップユニットと同期します。プライマリユニットに障害が発生した場合、バックアップユニットは中断することなくセッションの処理を継続します。」

質問: **37**
診断コマンドの部分的な出力を示す図を参照してください。



展示に示された出力から、どのような 2 つの結論を導き出すことができますか? (2 つ選択してください。)
A. これは、TCP ポートを動的に割り当てる TCP プロトコルのトラフィックを許可するピンホール セッションです。

B. FortiGate は、予想されるトラフィックが 23 秒以内に到着しない場合はそれをドロップします。
C. セッションはファイアウォール ポリシー ID 25 に対してチェックされます。
D. マスター セッションをクリアしても、期待セッションには影響しません。
正解: **(**正解を表示します**)**

質問: **38**
展示品を参照してください。
BGO デバッグ コマンドの出力が表示されます。

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60     4      65060    1698    1756        0    0    0 never       OpenSent
10.127.0.75     4      65060    2206    2250      102    0    0 02:45:55        0
100.64.3.1      4      65061     101     115        0    0    0 never       Active

Total number of neighbors 3
```

ローカル FortiGate が近隣からプレフィックスを受信しない最も可能性の高い理由は何ですか?
A. ローカル ルータは、ルータ 10.125.0.60 からのキープアライブ メッセージを待機しています。
B. 3 つのネイバーのいずれも、ローカル ルータとの TCP 3 ウェイ ハンドシェイクを正常に確立していません。
C. ルータ 100.64.3.1 は、ローカル ルータからの OPEN メッセージを待機しています。
D. ルータ 10.127.0.75 の RIB-OUT 構成により、ローカル ルータへのルート アドバタイズメントが防止されます。
正解: **D (**コメントを発表する**)**
プレフィックスが不足している理由を特定するには、get router info bgp summary の表示の State/PfxRcd 列と Up/Down 列を解釈する必要があります。
ネイバーステータスの分析:
ネイバー10.125.0.60: 状態はOpenSentです。このセッションは確立されていません。ネゴシエーションフェーズで停止しています。
ネイバー100.64.3.1: 状態はアクティブです。このセッションは確立されていません。ルータはTCP接続をアクティブに開始しようとしています。
近隣 10.127.0.75:
アップ/ダウン: 02:45:55。これは、BGPセッションが約3時間アップ（確立）状態あったことを示しています。
State/PfxRcd: 0。この数値は受信したプレフィックスの数を表します。セッションは完全に確立されていますが、ネイバーはルートを0件送信しています。
原因を特定する:

10.127.0.75 とのセッションが確立されているため、このネイバーでは接続とハンドシェイク (オプション A、B、C) に問題はありません。
アップ状態であるにもかかわらず、プレフィックスが 0 個送信されているという事実は、ネイバーがルートをローカル FortiGate に送信する前にそのルートをフィルタリングするように設定されていることを強く示唆しています。
オプション D は、これをネイバー (ルータ 10.127.0.75) の RIB-OUT (ルーティング情報ベース - アウトバウンド) 設定の問題として正しく識別し、そのルートのアドバタイズを妨げます。
参照：
FortiGate Security 7.6 学習ガイド (BGP): BGPサマリーで、State/PfxRcdに数字(例:
0の場合、セッションは確立されています。値が0の場合、ピアリングは確立されていますが、ルートが受信されていないことを意味します。これは、リモートピアでのルートマップまたはプレフィックスリストフィルタリングが原因であることが多いです。

質問: **39**
デバッグ方法を使用しているときに、iprope_in check() チェックが失敗し、ドロップする可能性がある 2 つの理由は何ですか?
（2つ選択してください。）
A. パケットはファイアウォール ポリシーによって許可されていないためドロップされました。
B. 送信元へのルートがないため、パケットはドロップされました。
C. 信頼できるホストリストの設定が誤っているため、パケットがドロップされました
D. 要求されたサービスがFortiGateで有効になっていないため、パケットはドロップされました
正解: **(**正解を表示します**)**
デバッグフローメッセージ「iprope_in_check() check failed, drop」は、Local-Inポリシーチェックの失敗を具体的に示しています。「iprope」(IP Routing Policy Enforcement）エンジンがポリシー検索を処理します。_in_check サフィックスは、この判定がFortiGate自体宛てのトラフィック（Local-Inトラフィック）に関するものであり、FortiGateを通過するトラフィックに関するものではないことを示しています。
D) 要求されたサービスがFortiGate上で有効になっていないため、パケットはドロップされました。
これが最も一般的な原因です。FortiGateのインターフェースIP宛てのパケット（例HTTPSまたはSSHリクエスト）が到着すると、カーネルはインターフェース設定（set allowaccess）で特定のサービスが有効になっているかどうかを確認します。サービスが有効になっていない場合（例PINGアクセスが無効になっているインターフェースにPINGを実行しようとする場合）、iprope_in_check関数は失敗し、パケットは直ちに破棄されます。
C) 信頼できるホスト リストが誤って設定されているため、パケットがドロップされました。
インターフェース上でサービス (HTTPS など) が有効になっている場合でも、FortiGate は管理者設定をチェックします。

信頼済みホストが設定されている場合、受信パケットの送信元IPが許可リストと照合されます。IPがリストにない場合、Local-Inポリシーチェック（prope_in_check）は失敗し、管理プレーンを保護するためにパケットはドロップされます。
他のオプションが間違っている理由:
A: 標準的なファイアウォールポリシーによってトラフィックがドロップされた場合（デバイスをあるインターフェースから別のインターフェースへ通過するトラフィック）、デバッグメッセージには通常、「ポリシーxによって拒否されました」または「一致するポリシーがありません」というメッセージが表示されます。これは通常、_in_checkではなく、forward check（prope_fwd_checkなど）です。
B: 送信元へのルートがない場合、エラーはリバースパスフォワーディング（RPF）の失敗です。デバッグフローでは、これを明示的に「リバースパスチェック失敗、ドロップ」としてログに記録します。
参照：
FortiGate トラブルシューティング ガイド (デバッグフロー): 「prope_in_check() チェック失敗」というメッセージは、パケットが Local-In ポリシーによって拒否されたことを示します。これは、FortiGate 宛てのトラフィックが allowaccess 設定によって許可されていないか、Trusted Host 設定によってブロックされている場合に発生します。

質問: **40**
セッション テーブル エントリの省略された出力を示す図を参照してください。

正しい記述はどれですか? (2 つ選択してください。)
A. セッションはオフロードされました。
B. トラフィックは VLAN 0000 にタグ付けされています。
C. トラフィックはポリシー ID 1 と一致します。
D. NP7 はこのセッションのオフロードを処理しています。
正解: **(正解を表示します)**

質問: **41**
セキュリティ ファブリックの通信に関する次の記述のうち、正しいものを 2 つ選択してください。
A. FortiTelemetry と Neighbor Discovery はどちらも TCP を使用して動作します。
B. 近隣探索のデフォルト ポートを変更できます。
C. FortiTelemetry は、FortiGate インターフェースで手動で有効にする必要があります。
D. デフォルトでは、ダウンストリーム FortiGate は TCP ポート 8013 を使用してアップストリーム FortiGate との接続を確立します。

正解: **C,D (**コメントを発表する**)**
FortiTelemetryはセキュリティファブリック通信の重要な部分であり、参加するFortiGateインターフェースごとに明示的な設定が必要です。管理アクセス設定（fabric」FortiTelemetryに対応）は、上流デバイスと下流デバイスの両方でインターフェースごとに手動で有効化する必要があります。これは、GUIの「管理アクセス」から、またはCLIの「set allowaccess fabric」コマンドを使用して、該当するネットワークインターフェースで実行できます。この手順を実行しないと、そのインターフェースでFortiTelemetry通信は行われません。
さらに、セキュリティ ファブリックにおける下流と上流の FortiGate ユニット間のデフォルトの通信は、TCP ポート 8013 経由で行われます。このポートは、セキュリティ ファブリックおよび FortiTelemetry 接続の標準として十分に文書化されており、ユニット間の接続とステータスの適用のために、ネットワーク パス全体で開いて許可されている必要があります。下流の FortiGate は、特に設定されていない限り、このポートを介して上流への接続を開始します。このポートは PCI 関連ポートとしても文書化されており、デフォルトの使用方法が示されています。
その他のオプション:
* FortiOS の近隣探索では、TCP ではなく IPv6 ND プロトコルが使用されます。
* FortiTelemetry ポート (8013) は変更できますが、セキュリティ ファブリックのインターフェース管理アクセスを手動で有効にする必要があります。ネイバー ディスカバリ ポートの変更は、FortiGate でサポートされている変更として文書化されていません。
参考文献:
FortiGate/FortiOS 管理ガイド: インターフェース上で FortiTelemetry (ファブリック) を有効にする Fortinet テクニカルヒント: FortiTelemetry はデフォルトで TCP ポート 8013 を使用します セキュリティファブリックにおけるポート 8013 の使用に関する PCI コンプライアンスドキュメント Fortinet セキュリティファブリックのセットアップ手順とインターフェースオプション

質問**: 42**
展示する。

IKE リアルタイム デバッグからの部分的な出力を含む展示を参照してください。
このデバッグ出力に関する次の 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. 構成で Perfect Forward Secrecy (PFS) が有効になっています。
B. ローカルゲートウェイの IP アドレスは 10.0.0.1 です。
C. フェーズ 2 のネゴシエーションを示します。
D. イニシエーターは IPsec ピア ID として remote を提供しました。
正解: **(正解を表示します)**
この図から、デバッグ出力がアグレッシブ モードで IKEv1 ネゴシエーションをキャプチャしていることがわかります。
公式の Fortinet IPsec VPN トラブルシューティング リソースとデバッグ ガイドに沿って、サポートの詳細を分析してみましょう。
オプションBの場合:
デバッグ出力の最初の行には次のように表示されます。
10.0.0.2:500->10.0.0.1:500、ifindex=7 になります。
これはトラフィックの方向、つまりリモートIP（10.0.0.2）のポート500からローカルIP（10.0.0.1）のポート500への方向を示しています。Fortinetのドキュメントによると、矢印の右側は常にローカルFortiGateゲートウェイを表します。したがって、10.0.0.1がローカルゲートウェイのIPアドレスとなります。
オプションDの場合:
次の文があります:
交渉結果『リモート」
そして
受信したピア識別子 FQDNCE88525E7DE7F00D6C2D3C00000000

公式のデバッグドキュメントでは、イニシエータから送信された「ピア識別子」またはピアIDがここに表示されると説明されています。IKE/IPsecネゴシエーションのコンテキストでは、この値は認証および識別のためのIPsecピアIDとして使用されます。イニシエータは、接続のピアIDとして「remote」を提供しています。
A や C ではない理由:
Perfect Forward Secrecy (PFS): デバッグではフェーズ 2 の DH グループ ネゴシエーションは表示されません (フェーズ 2 の group2、group5 などへの参照なし)。そのため、この出力からのみ PFS の存在を推測することはできません。
フェーズ 2 ネゴシエーション: ログは IKE (フェーズ 1) ネゴシエーションと確立に重点を置いています。フェーズ 2 SA ネゴシエーションと確立を示す ESP プロトコル、クイック モード、その他の識別子への参照はありません。
この解釈は、FortiOS 7.6.4管理ガイドのVPNセクションの説明と、Fortinetのドキュメントに掲載されている公式のデバッグコマンドの出力サンプルと一致しています。ローカルアドレスとリモートアドレスを区別する方法と、ピアIDの使用を識別する方法を示しています。
参考文献:
FortiOS 7.6.4 管理ガイド: IPsec VPN と VPN のデバッグ
IKEデバッグ出力とピアIDの役割の解釈に関するテクニカルサポートリソース

質問: **43**
展示品を参照してください。

```
# diagnose debug application fssod -1
# diagnose debug enable
[fsso_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO
workstation=, ip=10.124.2.90, port=49215, time=1372061722
```

fssodデーモンのリアルタイムデバッグコマンドの出力の一部を示します。この出力からどのような結論を導き出せますか？（2つ選択してください）
A. FSSO はユーザーがまだログインしているかどうかを確認できません。
B. Fortinet Single Sign-On (FSSO) は、DC エージェント モードを使用してログオン イベントを検出しています。
C. ユーザーがログアウトした場合に備えて、FortiGate はワークステーションを頻繁にポーリングしています。
D. FSSO はエージェントレス ポーリング モードを使用してログオン イベントを検出しています。
E. FortiGate は TCP ポート 8000 を介してこのイベントをポーリングしました。
正解: **(正解を表示します)**
デバッグ コマンド diagnose debug application fssod -1 は、FortiGate シングル サインオン デーモンの内部処理を明らかにします。
* オプションD（エージェントレスポーリング）：出力はevent_id=4768と表示されます。イベントID 4768（Kerberos TGT要求）はWindowsイベントログエントリです。fssodデバッグに一般的なロ

グオン通知ではなく特定のイベントIDが表示される場合、システムがドメインコントローラからセキュリティイベントログを読み取り（ポーリング）していることを示します。これは、FortiGateまたはコレクタがログをスクレイピングするエージェントレスポーリングモード（またはコレクタエージェントポーリングモード）の特徴です。一方、DCエージェントモードではログオン呼び出しが直接インターセプトされるため、通常はワークステーション名など、より詳細な情報が提供されます。
* オプションA（検証）：重要なのは、出力にworkstation=,と表示されていることです。これは、ワークステーション名フィールドが空であることを示しています。ポーリングモードでは、特定のイベントID（4768など）にソースワークステーションのホスト名が含まれていないことがよくあります。ワークステーション名がないと、FortiGate（またはコレクター）はワークステーションチェック（WMI/レジストリポーリング）を実行して、ユーザーがまだログインしているかどうかを確認することができません。ターゲットマシンの名前がないとアクティブな検証が不可能であるため、実質的に「デッドエントリタイムアウト」に頼らざるを得ません。
オプションBは不正解です。DCエージェントはワークステーション名を確実に取得します。オプションCは不正解です。システムは識別できないワークステーションをポーリングできないためです。

質問: **44**
FSSO コレクター エージェントから FortiGate に送信されるハートビート メッセージに関して正しい 2 つの記述はどれですか。
（2つ選択してください。）
A. ハートビート メッセージは、diagnose debug authd fsso list コマンドを使用して確認できます。
B. ハートビート メッセージは、コレクター エージェントのログに表示されます。
C. ハートビート メッセージは、リアル ライム FSSO デバッグを使用して FortiGate で確認できます。
D. ハートビート メッセージは FortiGate で手動で有効にする必要があります。
正解: **(正解を表示します)**
Fortinetの公式ドキュメント（テクニカルヒント：便利なFSSOコマンド）によると、ハートビートメッセージはFSSOコレクタエージェントとFortiGate間の通信において重要な役割を果たします。これらのメッセージは、コレクタエージェントから定期的に送信され、そのステータスの確認、セッション認識の維持、認証インフラストラクチャとFortiGateアプライアンス間の接続確認に使用されます。
オプション B は Fortinet によって確認されており、コレクター エージェントが Windows にログオンするか、その管理コンソールにハートビート イベント、接続ステータス、および FortiGate ユニットとの接続を維持する問題が具体的に記録されます。
オプションCは、公式CLIドキュメントとリンクされているテクニカルヒントの両方で検証されています。FortiGateでは、コレクタエージェントからのハートビートメッセージは、diagnose debug application authdなどのリアルタイムデバッグツールやFSSO固有のコマンドを使用して確認で

きます。これにより、管理者はFortiGate CLIから直接、ライブログオン状態、セッションステータス、接続の健全性を監視できます。デバッグストリームには、受信したハートビートとアクティブなログオンへの影響が表示され、健全性監視とアクティブセッションが関連付けられます。
FSSOの設定後、ハートビートの動作は完全に自動化されます。手動での有効化や設定は不要で、セキュリティファブリック全体にわたるシームレスな統合と集中管理というフォーティネットの理念に合致しています。これにより、FortiGateとコレクターエージェントの両方が、通信ミスや障害を迅速かつ確実に検知し、認証の問題にプロアクティブに対処できるようになります。
参考文献:
テクニカルヒント: 便利な FSSO コマンド (Fortinet コミュニティ)
FortiOS 管理ガイド: FSSO、コレクターエージェント、ハートビート、CLI デバッグ

質問: **45**
デバッグ方法を使用しているときに、iprope_in check() チェックが失敗し、ドロップする可能性がある 2 つの理由は何ですか?
(2つ選択してください。)
A. パケットはファイアウォール ポリシーによって許可されていないためドロップされました。
B. 送信元へのルートがないため、パケットはドロップされました。
C. 信頼できるホストリストの設定が誤っているため、パケットがドロップされました
D. 要求されたサービスがFortiGateで有効になっていないため、パケットはドロップされました
正解: **(正解を表示します)**
デバッグフローメッセージ「iprope_in_check() check failed, drop」は、Local-Inポリシーチェックの失敗を具体的に示しています。「iprope」(IP Routing Policy Enforcement)エンジンがポリシー検索を処理します。_in_check サフィックスは、この判定がFortiGate自体宛てのトラフィック(Local-Inトラフィック)に関するものであり、FortiGateを通過するトラフィックに関するものではないことを示しています。
* D. 要求されたサービスがFortiGateで有効になっていないため、パケットはドロップされました。
* 説明: これが最も一般的な原因です。FortiGateのインターフェースIP宛てのパケット(例:HTTPSまたはSSHリクエスト)が到着すると、カーネルはインターフェース設定(set allowaccess)で特定のサービスが有効になっているかどうかを確認します。サービスが有効になっていない場合(例:PINGアクセスが無効になっているインターフェースにPINGを実行しようとする場合)、iprope_in_check関数は失敗し、パケットは直ちに破棄されます。
* C. 信頼できるホスト リストが誤って設定されているため、パケットがドロップされました。
* 説明: インターフェース上でサービス(例:HTTPS)が有効になっている場合でも、FortiGateは管理者設定をチェックします。信頼済みホストが設定されている場合、受信パケットの送信元IPが許可リストと照合されます。IPがリストにない場合、Local-Inポリシーチェック(iprope_in_check)は失敗し、管理プレーンを保護するためにパケットはドロップされます。
他のオプションが間違っている理由:

* A: 標準的なファイアウォールポリシーによってトラフィックがドロップされた場合（デバイスをあるインターフェースから別のインターフェースへ通過するトラフィック）、デバッグメッセージには通常、「ポリシーxによって拒否されました」または「一致するポリシーがありません」というメッセージが表示されます。これは通常、_in_checkではなく、forward check（prope_fwd_checkなど）です。
* B: 送信元へのルートがない場合、エラーはリバースパスフォワーディング（RPF）の失敗です。デバッグフローでは、これを明示的に「リバースパスチェック失敗、ドロップ」としてログに記録します。
参照：
FortiGate トラブルシューティング ガイド (デバッグフロー): 「prope_in_check() チェック失敗」というメッセージは、パケットが Local-In ポリシーによって拒否されたことを示します。これは、FortiGate 宛てのトラフィックが allowaccess 設定によって許可されていないか、Trusted Host 設定によってブロックされている場合に発生します。

質問: **46**
IKEv2 では、どの交換が最初の CHILD_SA を確立しますか?
A. CREATE_CHILD_SA
B. 情報
C. IKE_認証
D. IKE_IN_HEAT
正解: **(**正解を表示します**)**

質問: **47**
展示する。

```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

診断自動化テストの出力を示す展示を参照してください。
出力から何が分かりますか? (2 つ選択してください。)
A. 自動化ステッチ テストは失敗しましたが、HA フェイルオーバーは成功しました。
B. 自動化ステッチ テストはログに記録されていません。

C. HA フェイルオーバーが発生しました。
D. テストは失敗しました。
正解: **(**正解を表示します**)**

質問: **48**
展示品を参照してください。

Diagnose output

```
# diagnose firewall proute list
list route policy info(vf=root):

id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=5(port3)
path(1): oif=6(port4) gwy=10.0.4.253
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 100.65.0.0/255.255.255.0
hit_count=0 rule_last_used=2025-04-29 15:56:55

# get router info routing-table  database
---omitted---
Routing table for VRF=0
O       10.0.4.0/24 [10/1] is directly connected, port4, 00:15:54, [1/0]
C    *> 10.0.4.0/24 is directly connected, port4
C    *> 10.0.5.0/24 is directly connected, port3
B       10.0.11.0/24 [10/0] via 10.0.11.254 inactive (recursive is directly connected, port2), 00:15:10, [1/0]
O       10.0.11.0/24 [10/1] is directly connected, port2, 00:15:54, [1/0]
C    *> 10.0.11.0/24 is directly connected, port2
B    *> 10.0.12.0/24 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
B    *> 10.0.13.0/24 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
B    *> 10.10.10.1/32 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
O       10.10.10.1/32 [10/1] via 10.0.11.254, port2, 00:15:29, [1/0]
S    *> 100.65.0.0/24 [10/0] via 10.0.11.253, port2, [1/0]
B       100.65.0.0/24 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
O       100.65.0.0/24 [10/2] via 10.0.11.254, port2, 00:15:29, [1/0]
B    *> 100.66.0.0/24 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
B       192.168.0.0/16 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
C    *> 192.168.0.0/16 is directly connected, port1
```

すべてのルートが同じ距離に設定されている場合、トラフィックはどのルートを経由して 100.65.0.0/24 ネットワークに到達しますか?
A. BGPルート
B. ポリシールート
C. 静的ルート
D. OS PFルート
正解: **(**正解を表示します**)**
トラフィックが通るパスを決定するには、FortiGate ルート ルックアップの優先順位 (パケット処理フロー) と、「ルーティングの優先順位の分析」の図に示されている特定の構成を確認する必要があります。
FortiOS では、パケットが到着すると (既存のセッションの一部ではない場合)、FortiGate は特定の順序でルート検索を実行します。
ポリシールート: config router policy または diagnose firewall proute list) で設定されます。これらは最初にチェックされます。パケットが基準（送信元 宛先、プロトコル、受信インターフェース）に一致する場合、標準ルーティングテーブルをバイパスして、ポリシールートが直ちに使用されます。
FIB (転送情報ベース): 一致するポリシー ルートがない場合、デバイスは標準ルーティング テーブル (静的、接続、動的) を参照します。
展示物を分析する:

ポリシー ルート セクション: diagnose firewall proute list の出力には、アクティブなポリシー ルート (id=1) が表示されます。
宛先: 100.65.0.0/255.255.255.0 (質問内のネットワークと一致します)。
アクション: トラフィックを oif=6 (ポート 4) 経由でゲートウェイ 10.0.4.253 に送信します。
ルーティングテーブルセクション: get router info routing-table databaseの出力には、100.65.0.0/24 (静的、OSPF、BGP)、すべて距離 10。FIB では現在、静的ルート (S) が選択されています (*>)。
結論：
ポリシー ルートは標準ルーティング テーブル (FIB) よりも優先されるため、FortiGate はポリシー ルート ID 1 の指示を使用してトラフィックを転送します。ポリシー ルートの基準 (入力ポート 3) に一致するトラフィックについては、ルーティング テーブルに表示される静的ルート、BGP ルート、または OSPF ルートは使用されません。
参照：
FortiGate Security 7.6 学習ガイド (ルーティング): ポリシー ルートは、ルーティング テーブル内のエントリよりも優先されます。
パケットがポリシー ルートに一致する場合、FortiGate は指定されたインターフェースとゲートウェイに従ってパケットをルーティングします。

質問: **49**
デバッグ出力を示す展示を参照してください。

```
# diagnose debug application authd 8256
# diagnose debug enable
....
[fsae_server_init_spec:116]: num 1, idx 0, 127.0.0.1:8000 disconnect_server_only
[FSSO]: disconnecting_event_error[Local FSSO Agent]: error occurred in read: Connection refused
....
```


管理者がDCエージェントモードでFSSOを導入しましたが、FortiGateでFSSOが失敗しています。コレクターエージェントが導入されている場所からFortiGateにpingを送信すると成功します。
次に、管理者は図に示すデバッグ出力を生成します。
このエラーメッセージの原因は何でしょうか?
A. FortiGate はアクティブ ディレクトリ サーバー名を解決できません。
B. コレクター エージェントの事前共有パスワードが一致しません。
C. FortiGate とコレクター エージェント間の TCP ポート 445 がブロックされています。
D. FortiGate とコレクター エージェントは異なる TCP ポートを使用しています。
正解: **(正解を表示します)**

質問: **50**
展示品を参照してください。

diagnose sys top コマンドはどの 3 つの情報を提供しますか? (3 つ選択してください。)

A. miglogd デーモンは CPU コア ID 0 で実行されています。

B. diagnose sys top コマンドが 18 分間実行されています。

C. 管理者がキーボードの m キーを押すと、miglogd デーモンがリストの一番上に表示されます。

D. cmdbsvr プロセスは、ユーザー メモリの合計領域の 2.4% を占有しています。

E. neweli デーモンが引き続き R 状態の場合は、手動で再起動する必要があります。

正解: **A,C,D** (コメントを発表する)

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-the-diagnose-sys-top-CLI-command/ta-p
/190238

質問: **51**

fssod デーモンのリアルタイム デバッグ コマンドの部分的な出力を示す展示を参照してください。

```
# diagnose debug application fssod -1
# diagnose debug enable
[fsso_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO workstation=, ip=10.124.2.90 port=49215, time=1372061722
```

出力からどのような 2 つの結論を導き出せますか? (2 つ選択してください。)

A. IP 10.124.2.90 のワークステーションは、ユーザーがまだログオンしているかどうかを確認するために、TCP ポート 445 を使用して頻繁にポーリングされます。

B. ログオン イベントは、Windows にインストールされたコレクター エージェントで確認できます。

C. FSSO は DC エージェント モードを使用してログオン イベントを検出しています。

D. FSSO はエージェントレス ポーリング モードを使用してログオン イベントを検出します。

正解: **(**正解を表示します**)**

質問: **52**

リアルタイム LDAP デバッグの部分的な出力を示す展示を参照してください。

```
# diagnose debug application fnbamd -1
# diagnose debug enable
fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
fnbamd_ldap.c[266] get_all_dn-Found DN: CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

出力からどのような 2 つの結論を導き出せますか? (2 つ選択してください。)

A. FortiOS はユーザー グループ情報を収集します。

B. FortiOS は、LDAP 認証プロセスの 2 番目のステップ (検索要求) を実行しています。

C. ユーザーは、ルートが TAC.ottawa.fortinet.com である LDAP ツリーで見つかりました。

D. FortiOS は、ユーザーの資格情報を使用して LDAP サーバーへのバインドを実行します。

正解: **(**正解を表示します**)**

質問: **53**

展示品を参照してください。

Debug output

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 av _idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=redir local may_dirty none app_ntf
statistic (bytes/packets/allow)err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
src mac=08:5b:0e: 6c:76:7a
misc=0 policy_ id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 to=ff/ff app_list=0 app=0 url_cat=41
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips offload=0/0, epid=0/0, ipid=0/0,vlan=0x0000/0
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

このセッションに関連する FortiGate の動作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. FortiGate は CPU を使用してセキュリティ プロファイル検査を実行しています。

B. FortiGateは、正しいポリシーマッチングができるように、クライアントをトリオキャプティブポータルにリダイレクトして認証しました。

C. FortiGate がセッションを開始したか、またはセッションが FortiGate で終了します。

D. FortiGate は検査なしでこのセッションを転送しました。

正解: **A,C (**コメントを発表する**)**

Fortinet FCSS - Network Security 7.6 ドキュメントとこれらの特定のトラブルシューティング シナリオの標準試験内容に基づいて、検証済みの回答を以下に示します。

質問: **54**
管理者が補助セッション販売を有効にした後、FortiGate はどのようなアクションを実行しますか? (2 つ選択してください。)
A. FortiGate は補助セッションのみをオフロードします。
B. FortiGateはNP6プロセッサへのすべてのECMPトラフィックを高速化します
C. FortiGates は、受信するパケットごとに補助セッションを作成します。
D. FortiGate はルーティングの変更に備えて 2 つのセッションを作成します。
正解: **(**正解を表示します**)**
「補助セッション」設定が有効になっている場合 (通常は config system npu 経由、または NP6/NP7 プロセッサ上の ECMP の場合は暗黙的に)、FortiGate はセッションの管理方法を変更し、インターフェースを切り替える可能性のあるトラフィック (ECMP や SD-WAN など) のハードウェア オフロードをサポートします。
B). FortiGate は NP6 プロセッサへのすべての ECMP トラフィックを高速化します。
補助セッションを有効にする主な目的は、ECMPトラフィックをNPUによって完全にオフロード（高速化）できるようにすることです。補助セッションがない場合、カーネルまたはルーティングエンジンが（ロードバランシングのために）フローを別の出力インターフェースに切り替えた場合、NPUはその新しいインターフェースのフローを認識できず、パケットをCPU（低速パス）に送り返す可能性があります。補助セッションは、すべての有効なパスに関する必要な情報をNPUに事前に設定することで、このような事態を防ぎます。
D). FortiGate はルーティングが変更された場合に 2 つのセッションを作成します。
技術的には、FortiGateはプライマリセッション（現在選択されているパス用）と補助セッション（代替パス用）を作成します。標準的な2パスECMPシナリオでは、これにより、同じフローに対してセッションテーブルに「2つのセッション」が存在することになります。これにより、ルーティングの変更（例えば、フローが2番目のパスにシフトする）が発生しても、トラフィックはCPUによる中断や再評価なしに、NPUによって処理され続けます。

質問: **55**
ルーティング カーネルの変更された出力を示す展示を参照してください。

どちらの記述が正しいでしょうか?

A. 10.200.1.254 を経由するデフォルトの静的ルートが転送情報ベースにありません。

B. 10.0.4.0/24 への BGP ルートが転送情報ベースにありません。

C. ポート2 を経由するデフォルトの静的ルートは、転送情報ベースにあります。

D. 静的ルート 8.8.8.8/32 に関連付けられた出力インターフェイスは管理上アップしています。

正解: **(**正解を表示します**)**

質問: **56**

OSPF ルータのリンク ステイル データベース (LSD6) にタイプ 5 のタンクの状態通知 (LSA) がまったく含まれない 2 つの理由は何ですか (2 つ選択してください)。

A. ネットワーク内に自律システム境界ルータ (ASBR) が存在しません。

B. ローカル ルータのピアは、prefix-list-out 設定を使用して、すべてのタイプ 5 LSA がアドバタイズされるのを防止しています。

C. ローカルルータはスタブエリアに位置している

D. IP プロトコル 89 は、ローカル ルータとそのピア間でブロックされています。

正解: **(**正解を表示します**)**

タイプ 5 LSA (AS 外部 LSA) がリンクステート データベース (LSDB) に存在しない理由を理解するには、OSPF がそれらを生成して伝播する方法を確認する必要があります。

* A. ネットワーク内に自律システム境界ルータ (ASBR) が存在しません。

* 理由: タイプ5 LSAは、他のプロトコル (スタティック、BGP、RIPなど) からOSPFドメインに再配布されたルートをアドバタイズするために、ASBRによってのみ生成されます。外部ルートを再配布するように設定されたルータ (ASBRとして機能するルータ) がない場合、そもそもタイプ5 LSAは作成されません。

* C. ローカルルータはスタブエリアにあります。

* 理由: 定義上、スタブエリア (および完全スタブエリア) はタイプ5 LSAの進入をブロックします。スタブエリアをバックボーンに接続するエリア境界ルータ (ABR) は、すべてのタイプ5 LSAを

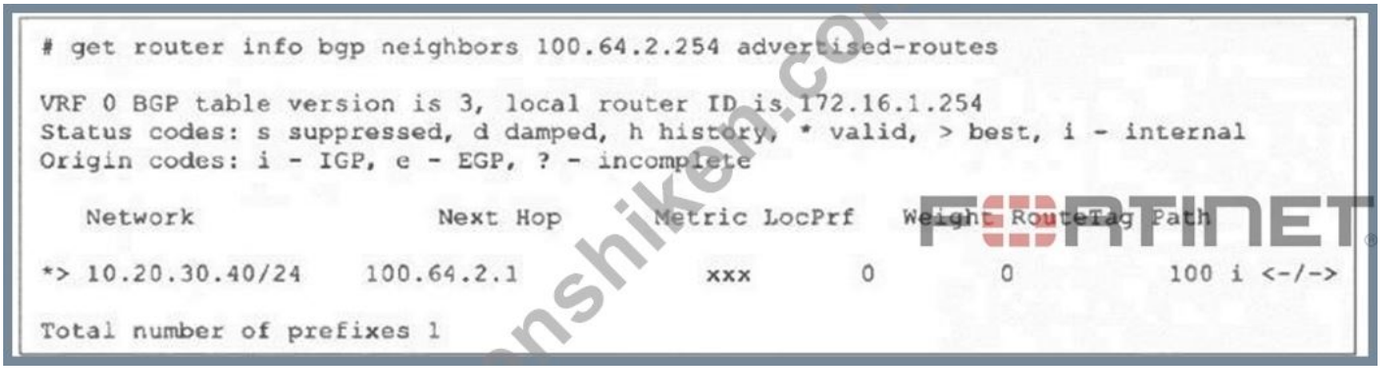
フィルタリングすることで、そのエリア内のルータのLSDBとルーティングテーブルのサイズを削減します。
代わりに、通常はデフォルトのルートが挿入されます。
* 他の選択肢が間違っている理由:
* B: データベース フィルタリングは存在しますが、標準のプレフィックス リスト フィルタリングは通常、ルーティング テーブル (RIB) の生成に影響し、Type 5 LSA の基礎となる LSDB 伝播には影響しません。または、アーキテクチャ上の理由 (スタブ/ASBR なし) よりも一般的ではありません。
* D: IPプロトコル89はOSPF自体のトランスポートです。これがブロックされると、OSPF隣接関係は全く形成されず、ルータはタイプ5だけでなく、タイプ1、2などのLSAを一切受信できなくなります。
参照：
FortiGate セキュリティ 7.6 学習ガイド (OSPF): タイプ 5 LSA は ASBR によって生成されます... スタブ エリアではタイプ 5 LSA は許可されず、デフォルト ルートに置き換えられます。」

質問: **57**
セッション テーブル エントリの省略された出力を示す図を参照してください。

正しい記述はどれですか? (2 つ選択してください。)
A. トラフィックは VLAN 0000 にタグ付けされています。
B. NP7 はこのセッションのオフロードを処理しています。
C. トラフィックはポリシー ID 1 と一致します。
D. セッションはオフロードされました。
正解: **C,D (**コメントを発表する**)**
提供されたセッション テーブル出力では、次の詳細が回答の根拠となっています。
ポリシーIDの一致: policy_id=1の行は、このセッションがファイアウォールポリシーIDと一致したことを直接確認します。
1. Fortinet のセッション テーブルのドキュメントによると、policy_id フィールドは常にこのセッションを許可したポリシーを参照するため、これは明確な指標となります。
セッションオフロード：文字列pu_state、ips_offload、そして特にoffload=8/8、ips_offload=1/1といったNPU情報セクションの存在は、このセッションがネットワークプロセッサユニット（NPU）にオフロードされていることを示しています。Fortinetの技術文書によると、両方向の「オフロード」値が0より大きいこと（およびNPU情報セクション）は、NPUハードウェア処理（高速パス）がこのトラフィックを処理していることを示しており、セッションがソフトウェアのみで処理されているわけではないことを示しています。
その他のオプション:

VLAN タグ付け (vlan=0x0000/0x0000): これは、このセッションに VLAN タグが割り当てられていないことを意味します。
NP7: セッションを処理する実際の NPU モデルはこのスニペットでは公開されません。表示されるオフロード パラメーターは汎用的なものであり、NP7 ハードウェアに固有のものではないため、セッション データから結論付けることはできません。
参考文献:
Fortinet のテクニカルヒント: FortiGate セッション テーブルと NPU オフロード
FortiOS 診断ガイド: ポリシー ID、オフロード、VLAN セッション テーブル フィールド

質問: **58**
コマンド get router info bgp neighbors 100.64.2.254 advertised-routes の出力を示す図を参照してください。


```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24    100.64.2.1               xxx       0        0          100 i <-/->

Total number of prefixes 1
```

出力から何を結論づけることができますか?
A. ローカル ルータは、10.20.30.40/24 ネットワークを BGP ネイバーにアドバタイズしています。
B. ネイバーのルータ ID は 100.64.2.254 です。
C. BGP ネイバーは 10.20.30.40/24 ネットワークをローカル ルータにアドバタイズしています。
D. 2 つの BGP 参加者の BGP 状態は OpenConfirm です。
正解: **A** (コメントを発表する)

質問: **59**
デバッグ出力を示す展示を参照してください。


```
# diagnose debug application authd 8256
# diagnose debug enable
....
[fsae_server_init_spec:116]: num 1, idx 0, 127.0.0.1:8000 disconnect_server_only
[FSSO]: disconnecting_event_error[Local FSSO Agent]: error occurred in read: Connection refused
....
```

管理者がDCエージェントモードでFSSOを導入しましたが、FortiGateでFSSOが失敗しています。コレクターエージェントが導入されている場所からFortiGateにpingを送信すると成功します。
次に、管理者は図に示すデバッグ出力を生成します。
このエラーメッセージの原因は何でしょうか?
A. FortiGate はアクティブ ディレクトリ サーバー名を解決できません。

B. FortiGate とコレクター エージェント間の TCP ポート 445 がブロックされています。
C. FortiGate とコレクター エージェントは異なる TCP ポートを使用しています。
D. コレクター エージェントの事前共有パスワードが一致しません。
正解: **(**正解を表示します**)**

質問: **60**
FortiOS カーネル スラブの部分的な出力を示す展示を参照してください。

```
...
packet_de_duplication    0    0    128    30    1 : tunables  252  126    0 : slabdata    0    0    0
ip6_nat_record           0    0    128    30    1 : tunables  252  126    0 : slabdata    0    0    0
tcp6_session             0    0   1536     5    2 : tunables   60   30    0 : slabdata    0    0    0
ip6_session              0    0   1300     3    1 : tunables   60   30    0 : slabdata    0    0    0
ip_nat_record            0    0     64    59    1 : tunables  252  126    0 : slabdata    0    0    0
sctp_session             0    0   1600     5    2 : tunables   60   30    0 : slabdata    0    0    0
tcp_session              3    5   1500     5    2 : tunables   60   30    0 : slabdata    1    1    0
ip_session               1    3   1200     3    1 : tunables   60   30    0 : slabdata    1    1    0
...
```

どちらの記述が正しいでしょうか?
A. sctp_session スラブの合計スラブ サイズは 0 kB で、ユーザー スペースに関連付けられています。
B. ip_session スラブの合計スラブ サイズは 3600 kB で、ユーザー スペースに関連付けられています。
C. tcp_session スラブの合計スラブ サイズは 7500 kB で、カーネルに関連付けられています。
D. ip6_session スラブの合計スラブ サイズは 1300 kB で、カーネルに関連付けられています。
正解: **C (**コメントを発表する**)**

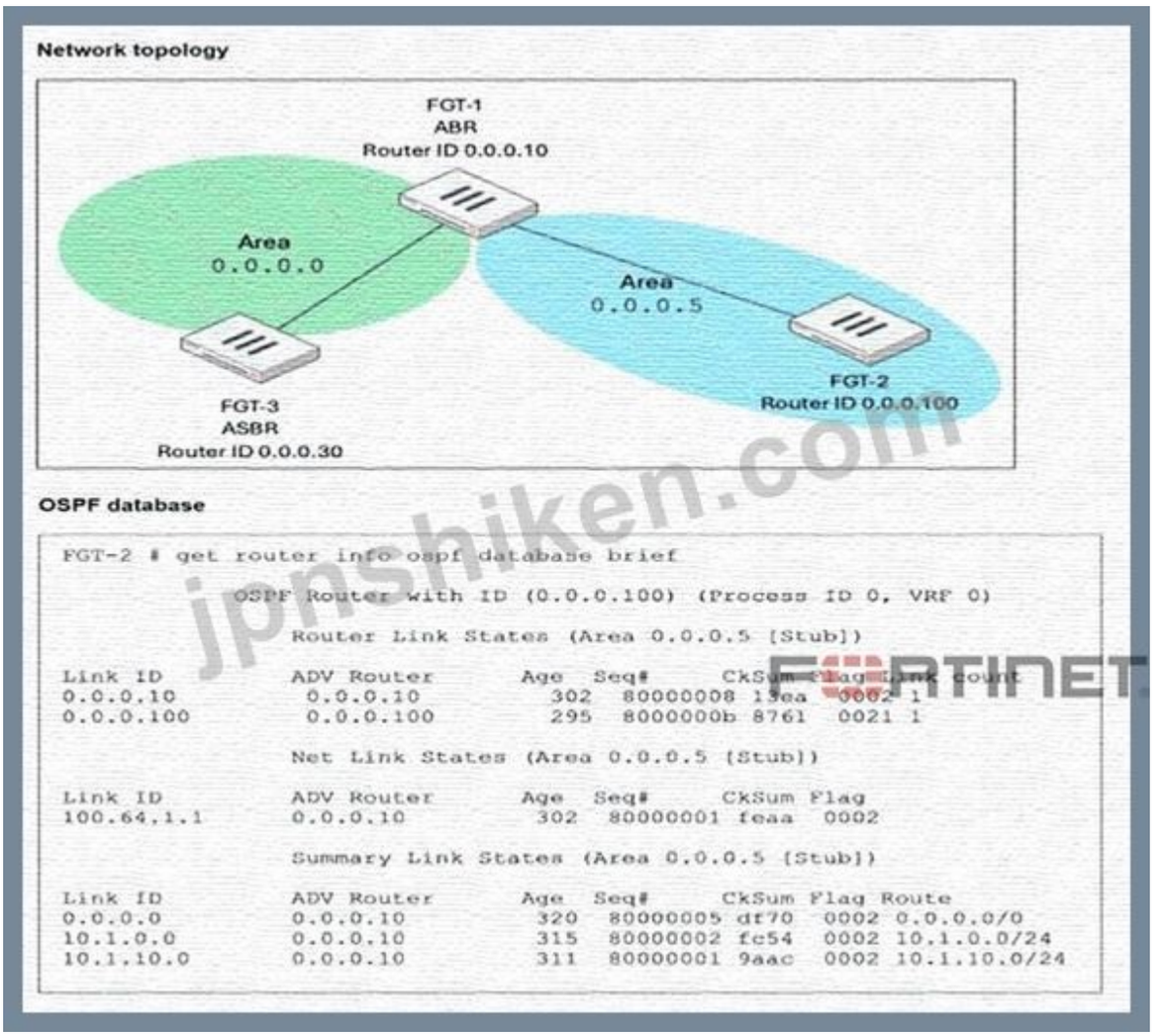
質問: **61**
リアルタイム LDAP デバッグの切り捨てられた出力を示す展示を参照してください。

```
# diagnose debug application fnbamd -1
# diagnose debug enable
  fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
  fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
  fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
  fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
  fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
  fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

出力からどのような 2 つの結論を導き出せますか? (2 つ選択してください。)
A. 構成された LDAP サーバーの名前は Lab です。
B. ユーザーは CN=John Smith を使用して認証しています。
C. FortiOS は、LDAP 認証プロセスのステップ 3 (バインド要求) でユーザーを見つけることができます。
D. FortiOS は、LDAP 認証プロセスの 2 番目のステップ (検索要求) を実行しています。
正解: **(**正解を表示します**)**
FortiOS管理ガイドに記載されているFortinetのLDAP認証ワークフローと公式LDAPデバッグログの解釈によると、各認証試行は複数の主要なステップに分割されます。バインド要求、検索要求、そして成功した場合は見つかったユーザーDNでのバインドです。提供されたデバッグ出力には、「start search_dn-base」とフィルター「sAMAccountName=jsmith」、そしてログ行「Going to

SEARCH state」が表示されており、FortiOSが2番目のステップである検索要求（オプションD）にあることが確認できます。公式ドキュメントでは、この「SEARCH state」というフレーズがLDAPプロセスのステップ2（「Bind # Search # Bind」）を示すものとして強調されています。
さらに、最後の行「Found DN 1: CN=John Smith, CN=Users, DC=TAC, DC=ottawa, DC=fortinet, DC=com」は、システムがユーザー名を識別名（DN）に正常にマッピングし、このユーザーが「John Smith」であることを確認しています。認証は、このマッピングされたユーザーを使用して続行されます（オプションB）。
Fortinet のログには、検索が成功すると見つかった DN が記録されます。これは、見つかった DN に対してユーザーの資格情報が検証できることを強力に証明します。
オプション A と C は、示されているデバッグ出力では直接サポートされていません。
* サーバー名「lab」はリクエストの一部として参照されますが、この出力では LDAP サーバーの構成名として明示的に参照されるわけではありません。
* ステップ 3 (バインド要求) は DN の検索に続きますが、ここでのログは Fortinet に従って検索と DN が見つかったことを示し、これは実際のバインド/検証ステップの前に行われます。
参考文献:
FortiOS 管理ガイド: LDAP 認証プロセスとデバッグログ Fortinet 公式 KB: LDAP 統合ワークフローとログの解釈

質問: **62**
展示物を参照してください。



FGT-1は、OSPFエリア0.0.0.0と0.0.0.5にインターフェースを持つエリア境界ルータ（ABR）です。FGT-3は自律システム境界ルータ（ASBR）として機能し、スタティックルートをOSPFにインポートします。FGT-2は、すべてのインターフェースがエリア0.0.0.5に属する内部ルータです。FGT-1はFGT-2からアドバタイズされたすべてのルートを受信していますが、FGT-3はFGT-1からアドバタイズされたルートを全く受信していません。この原因として最も考えられるものは何でしょうか？

（1つ選択してください）

A. エリア 0.0.0.5 は、タイプ 5 LSA を伝播しないように設定されています。

B. FGT-2 は、FGT-3 からのすべてのアドバタイズされたルートをブロックする配布リストを使用して設定されています。

C. FGT-3 と FGT-2 はまだ OSPF 隣接関係を形成していません。

D. IP プロトコル 89 は FGT-1 と FGT-3 の間でブロックされています。

正解: **A** (コメントを発表する)

ネットワークセキュリティの正確な抜粋からの包括的かつ詳細な150～200語の説明

7.6 ドキュメント:

FGT-2のget router info ospf database briefの出力は、エリア0.0.0.5が次のように設定されていることを明確に示しています。

[スタブ]エリア。

OSPFにおいて、スタブエリアは内部ルータのリンクステートデータベース（LSDB）のサイズを削減するために特別に設計されています。スタブエリアの主な動作は、タイプ5（AS外部）LSAを受け入れないことです。
* FGT-3 は ASBR (自律システム境界ルータ) であり、OSPF ドメインでタイプ 5 LSA として生成される静的ルートをインポートします。
* FGT-1はABR（エリア境界ルータ）として機能します。エリア0.0.0.5はスタブエリアであるため、FGT-1はこれらのタイプ5 LSAがエリア0.0.0.5に入るのをブロックします。
* その結果、FGT-2はFGT-3によってアドバタイズされた特定の外部ルートを受信しません。代わりに、ABR（FGT-1）はデフォルトルート（0.0.0.0/0）をスタブエリアに挿入し、外部への接続を許可します。これはデータベース出力に表示されます。
質問のテキストでは FGT-3 がルートを受信しないと述べられていますが、図に示されている決定的な構成はスタブ エリア設定であり、これはタイプ 5 LSA 伝播のブロック (オプション A) に直接対応しています。

質問: **63**
展示品を参照してください。

```
FGT-01
#diagnose sniffer packet any 'esp' 4
2024-03-07 15:57:40.344931 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415b)
2024-03-07 15:57:40.344949 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415c)
2024-03-07 15:57:40.344974 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415d)
2024-03-07 15:57:40.346832 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415e)
2024-03-07 15:57:40.347463 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415f)

FGT-02
#diagnose sniffer packet any 'esp' 4
(no packets captured)
```


2台のFortiGateデバイスのスニファーログが表示されています。ログの情報に基づいて、FortiGate FGT-02の出力を説明する2つの要因は何ですか？（2つ選択してください）
A. サードパーティのデバイスがプロトコル 50 をブロックしています。
B. 管理者は FGT-02 上で VPN トンネルをまだ設定していません。
C. 管理者が FGT-01 に間違ったリモート ピア IP アドレスを設定しました。
D. 管理者が FGT-02 に間違ったスニファー フィルターを設定しました。
正解: **(**正解を表示します**)**
ネットワークセキュリティの正確な抜粋からの包括的かつ詳細な150〜200語の説明
7.6 ドキュメント:
FGT-01の出力から、デバイスがトラフィックをカプセル化し、ESPパケット（プロトコル50）としてポート1からIPアドレス97.86.16.52に向けて送信していることが確認できます。ログには送信パケットが表示されており、FGT-01がトンネルの開始または維持を試みていること、そしてNATトラバーサルが使用されていないこと（raw ESPを使用しているため）が確認できます。

しかし、FGT-02の出力には「パケットがキャプチャされていません」と表示されています。これは重要な意味を持ちます。なぜなら、スニファーコマンド「diagnose sniffer packet any 'esp'」は、受信側ユニットに一致するVPN設定が存在するかどうかに関係なく、ネットワークインターフェースレベル（入力）でトラフィックをキャプチャするからです。パケットが存在しないことは、FGT-01によって生成されたESPトラフィックが物理的にFGT-02のインターフェースに到達していないことを示しています。
この動作は、主に次の 2 つの要因によって説明されます。
* オプションA（ブロッキング）ISPルーターやファイアウォールなどの中間デバイスがプロトコル
をドロップしている
50 トラフィック。UDP 500/4500 とは異なり、多くのネットワークやレガシーデバイスでは、raw ESP はデフォルトでブロックされることがよくあります。
* オプションC（ルーティング/設定ミス）：管理者がFGT-01のリモートピアIPアドレスを誤って設定した場合、パケットは全く別の宛先にルーティングされます。その結果、パケットはFGT-02に到達せず、キャプチャされません。
オプションBは誤りです。VPNトンネルが設定されていない場合でも、インターフェースに到達したESPパケットはスニファーに表示されるからです。オプションDは誤りです。FGT-01がESPを送信しているため、「esp」が適切なフィルターとなります。

質問: **64**
展示する。

FortiGate の構成を示す展示を参照してください。

管理者はFortiGateのWebフィルタに関する問題をトラブルシューティングしています。管理者はWebフィルタプロファイルを設定し、ポリシーに適用しましたが、Webフィルタはポリシーを通過するトラフィックを検査していません。

問題を解決するために管理者は何をする必要がありますか?

A. webfilter-force-off を無効にします。

B. Fortiguard-anycast を有効にします。

C. Web フィルターのタイムアウトを増やします。

D. プロトコルを TCP に変更します。

正解: **(**正解を表示します**)**

質問: **65**

展示品を参照してください。

展示ではセッションのエントリを示します。

この TCP セッションに関する正しい記述はどれですか?

A. セッションは NP7 を使用してオフロードされます。

B. イニシエーターへの戻りトラフィックは

C. 10.9.31.117から10.1.0.3へのTCPセッションです

D. セッションは 1 秒後に期限切れになります。

正解: **(正解を表示します)**

正しい記述を判断するには、図に示されている diagnose sys session list 出力内の特定のフィールドを分析する必要があります。

* オプション A を分析します (セッションは NP7 を使用してオフロードされます)。

* 証拠: キーインジケーターは、npu info: flag=0x81/0x81、offload=8/8、ips_offload=1/1 の行です。

* 説明: この特定の npu 情報出力形式、特に offload=8/8 および ips_offload=1/1 カウンタは、NP7 (ネットワーク プロセッサ 7) アクセラレーションの特徴です。

* 従来のNP6プロセッサは通常、np6_0フラグまたは異なるオフロード状態ビットマップを表示します。NP7アーキテクチャは、IPS（侵入防止システム）処理を含むセッションの完全なハードウェアオフロードをサポートしており、ここではips_offloadとして明示的に示されています。offload=8/8は、元の方向と応答方向の両方がNPUに完全にオフロードされていることを示します。

* オプション C を分析します (10.9.31.117 から 10.1.0.3 への TCP セッションです):

* 証拠: hook=post 行は SNAT 変換を示しています: 10.9.31.117:45388->200.8.57.5:443 (10.1.0.3:45388)。

* 説明 :

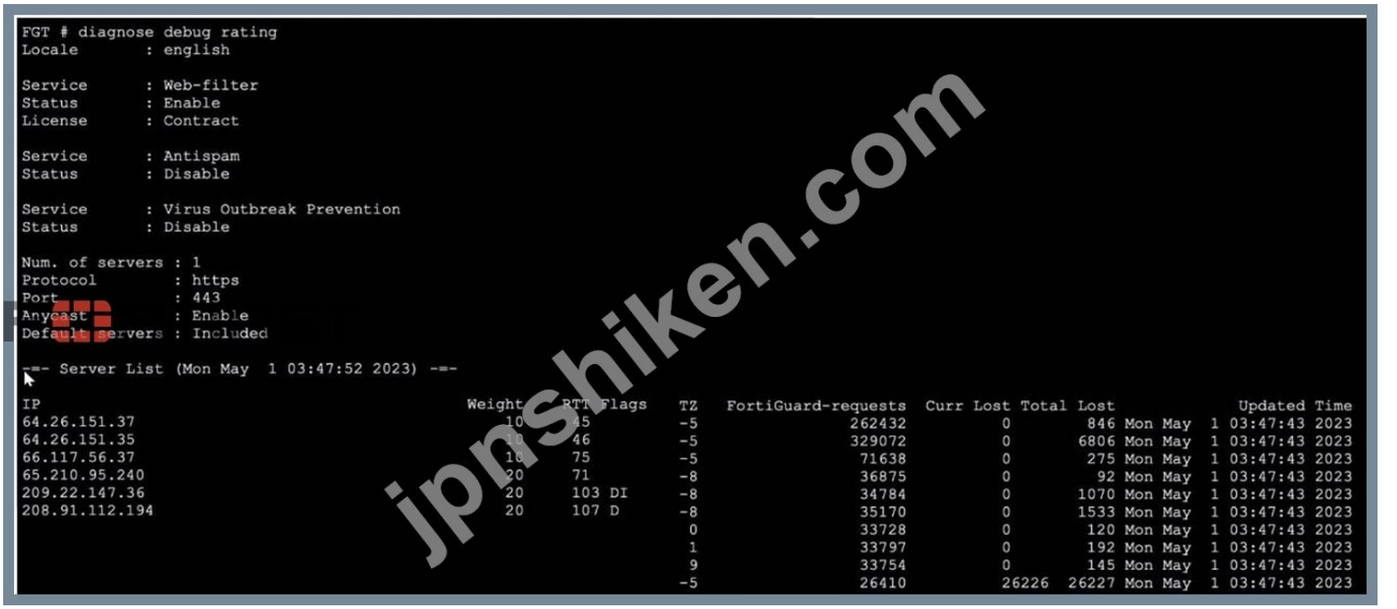
* ソース: 10.9.31.117 (クライアント)。

* 宛先: 200.8.57.5 (ポート 443 の外部サーバー)。

* NAT IP: 10.1.0.3 は、トラフィックがインターフェースから送信される際に FortiGate が送信元 NAT (SNAT) に使用する IP アドレスです。これはセッションの宛先ではありません。

* 結論: この記述は誤りです。
* オプション D を分析します (セッションは 1 秒後に期限切れになります):
* 証拠: セッション情報行に、expire=3599 と表示されます。
* 説明: 有効期限カウンタは、セッションが削除されるまでの残り秒数を示します（これ以上パケットが送信されない場合）。値が3599秒の場合、セッションは更新されたばかり（おそらく3600秒のタイムアウト）であり、1秒ではなく約1時間後に有効期限が切れます。
* 結論: この記述は誤りです。
* オプション B を分析します (イニシエーターへの戻りトラフィックは... に送信されます)。
* 応答トラフィックのゲートウェイ (gwy=.../10.9.31.117) は戻りトラフィックがその IP に送信されることを示していますが、オプション A は、この試験モジュールでテストされるハードウェアアーキテクチャ (NP7) に関する決定的な技術的観察を提供します。
参照：
FortiGate Security 7.6 学習ガイド (ハードウェア アクセラレーション): 「NP7 プラットフォームでは、diagnose sys session list コマンドに npu info 行が含まれます。offload=8/8 は、セッションが完全にオフロードされていることを示します。
ips_offload は、NPU 上の IPS エンジンがトラフィックを検査していることを示します。

質問**: 66**
展示する。



診断コマンドの出力を示す展示を参照してください。
このシナリオのデバッグ出力についてどのような結論を導き出せますか?
A. 評価サーバーのリストを検索する DNS クエリを実行したときに FortiGate に提供された最初のサーバーは 121.111.236.179 でした。
B. FortiGuard-requests フィールドの値と Weight フィールドの値の間には自然な相関関係があります。
C. FortiGate は、契約を検証するための初期サーバーとして 64.26.151.37 を使用しました。
D. 負の TZ 値を持つサーバーは、評価リクエストに対してあまり優先されません。

正解: (正解を表示します)
この図は、FortiGateデバイスにおけるdiagnose debug ratingコマンドの出力を示しています。このコマンドは、FortiGuard Webフィルタリングや、FortiGateがFortiGuardサーバーに対して実行するその他のセキュリティ関連クエリに関する情報を表示するために使用されます。サーバーリストの各フィールドの意味については、フォーティネットの公式ドキュメントをご覧ください。FortiGateは利用可能なFortiGuardサーバーのリストを保持しており、重み付け、ラウンドトリップ時間（RTT）、地域設定などの要素に基づいて最適なサーバーを選択します。
「サーバーリスト」の後のサーバーリストの一番最初のエントリは、FortiGateが最初に使用するサーバーで、近接性やRTTなどの要素に基づいて優先順位が付けられています。ここでは64.26.151.37が最初にリストされており、FortiGuard-requestsの値から、このサーバーが最も多くのリクエストを処理したことが分かります。
IP、重み、および損失/失敗カウンターは、時間の経過に伴うサーバーのパフォーマンスと選択のために監視されます。
FortiGate のデフォルトの動作ロジックでは、契約の検証に最初のエントリを試行し、最初のエントリが利用できないか、遅延やパケット損失が大きい場合は、リスト内の次のエントリを使用します。
重みとFortiGuardリクエスト数の間には直接的な相関関係はありません。重みが高いサーバーや低いサーバーでは、可用性とパフォーマンスに応じて、処理できるリクエスト量が異なる場合があります。
TZ (タイム ゾーン) 値の符号 (正または負) は、サーバー設定に影響しません。これは、UTC を基準としたサーバーの位置を示す情報であり、評価基準ではありません。
FortiGuard サーバーの DNS クエリ結果はここには表示されず、提供されたサーバーは DNS クエリの順序で返されません。
このコマンドと解釈については、FortiOS 管理ガイドの FortiGuard サーバーの選択と契約検証プロセスについて説明しているセクションで詳しく説明されています。
参考文献:
FortiOS管理ガイド: FortiGuardサービスの接続とデバッグ診断デバッグ評価出力構造に関する公式テクニカルノート

質問: **67**
SAML ネゴシエーション プロセスでは、どのセクションで、アイデンティティ プロバイダー (IdP) が認証プロセスで使用される SAML 属性をサービス プロバイダー (SP) に提供しますか。
A. SP ログインダンプ
B. アサーションダンプ
C. 認証レスポンス
D. 認証リクエスト
正解: (正解を表示します)

質問: **68**

展示する。

IKE リアルタイム デバッグからの部分的な出力を含む展示を参照してください。

このデバッグ出力に関する次の 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. イニシエーターは IPsec ピア ID として remote を提供しました。

B. ローカルゲートウェイの IP アドレスは 10.0.0.1 です。

C. 構成で Perfect Forward Secrecy (PFS) が有効になっています。

D. フェーズ 2 のネゴシエーションを示します。

正解: **(**正解を表示します**)**

質問: **69**

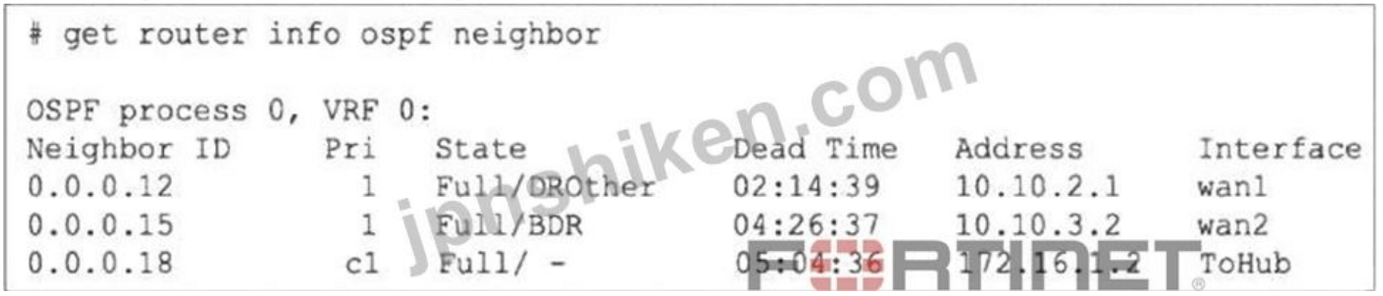
展示品を参照してください。

展示ではセッションのエントリを示します。

この TCP セッションに関する正しい記述はどれですか?
A. セッションは NP7 を使用してオフロードされます。
B. イニシエーターへの戻りトラフィックは
C. 10.9.31.117から10.1.0.3へのTCPセッションです
D. セッションは 1 秒後に期限切れになります。
正解**: (**正解を表示します**)**
正しい記述を判断するには、図に示されている diagnose sys session list 出力内の特定のフィールドを分析する必要があります。
オプション A を分析します (セッションは NP7 を使用してオフロードされます)。
証拠: キーインジケーターは、npu info: flag=0x81/0x81、offload=8/8、ips_offload=1/1 の行です。
この特定の npu info 出力形式、特に offload=8/8 および ips_offload=1/1 カウンタは、NP7 (ネットワーク プロセッサ 7) アクセラレーションの特徴です。
従来のNP6プロセッサは通常、np6_0フラグまたは異なるオフロード状態ビットマップを表示します。NP7アーキテクチャは、IPS（侵入防止システム）処理を含むセッションの完全なハードウェアオフロードをサポートしており、ここではips_offloadとして明示的に示されています。offload=8/8は、元の方向と応答方向の両方がNPUに完全にオフロードされていることを示します。
オプション C を分析します (10.9.31.117 から 10.1.0.3 への TCP セッションです)。
証拠: hook=post 行は SNAT 変換を示しています: 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)。
ソース: 10.9.31.117 (クライアント)。
宛先: 200.8.57.5 (ポート 443 の外部サーバー)。
NAT IP: 10.1.0.3 は、トラフィックがインターフェースから送信されるときに FortiGate がソース NAT (SNAT) に使用する IP アドレスです。
セッションの宛先ではありません。
結論: この記述は誤りです。
オプション D を分析します (セッションは 1 秒後に期限切れになります)。
証拠: セッション情報行に、expire=3599 と表示されます。
有効期限カウンタは、セッションが削除されるまでの残り秒数を示します（これ以上パケットが送信されない場合）。値が3599秒の場合、セッションは更新されたばかり（おそらく3600秒のタイムアウト）であり、1秒ではなく約1時間後に有効期限が切れます。
結論: この記述は誤りです。
オプション B を分析します (イニシエーターへの戻りトラフィックは... に送信されます)。
応答トラフィックのゲートウェイ (gwy=.../10.9.31.117) は戻りトラフィックがその IP に送信されることを示していますが、オプション A は、この試験モジュールでテストされるハードウェアアーキテクチャ (NP7) に関する決定的な技術的観察を提供します。
参照：
FortiGate Security 7.6 学習ガイド (ハードウェア アクセラレーション): 「NP7 プラットフォームでは、diagnose sys session list コマンドに npu info 行が含まれます。offload=8/8 は、セッション

が完全にオフロードされていることを示します。ips_offload は、NPU 上の IPS エンジンがトラフィックを検査していることを示します。」

質問: **70**
コマンド get router info ospf neighbor の出力を示す図を参照してください。



FortiGate は OSPF ネイバーを確認する際にどの程度動作しますか? (2 つ選択してください。)
A. ローカル FortiGate には、ブロードキャスト ネットワークに参加するインターフェースが少なくとも 1 つあります。
B. ローカル FortiGate には、ポイントツーポイント ネットワークに参加するインターフェースが少なくとも 1 つあります。
C. ローカル FortiGate が DR です。
D. ネイバー 0.0.0.18 は指定ルータ (DR) です。
正解: **(**正解を表示します**)**
このスライドのコマンドは、すべてのOSPFネイバーのステータスの概要を表示します。ネイバーごとに、隣接関係の状態と、DR、BDR、またはどちらでもない（DROther）が表示されます（Pagina 362 Enterprise_Firewall_7）。
2_Study. - ポイントツーポイントネットワークは、ポイントツーポイントリンクの両端に1つずつ、合計2つのピアのみで構成されます。- ブロードキャストネットワーク（マルチアクセス）は、2台以上の接続されたルータをサポートします。また、複数の受信者へのメッセージ送信（ブロードキャスト）もサポートします。Pagina 365 Enterprise_Firewall_7.2_Study. どのマルチアクセスネットワークにも、1つのDRと1つのBDRが存在します。Pagina 439 Network_Security_Support_Engineer_7.4_Study FULL/- これはポイントツーポイントネットワークを表しています。