Fortinet.FCSS_NST_SE-7.6.v2026-07-29.q105

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：	105
バージョン：	v2026-07-29
ページの閲覧量：	104
問題集の閲覧量：	1189

https://www.jpnshiken.com/shiken/Fortinet.FCSS_NST_SE-7.6.v2026-07-29.q105.html

質問: **1**

図を参照してください。図には、BGPデバッグコマンドの出力結果が示されています。

```
# 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      103    0    0 03:02:49        1
10.127.0.75     4      65075    2206    2250      102    0    0 02:45:55        1
100.64.3.1      4      65501     101     115        0    0    0 never       Active

Total number of neighbors 3
```

この状況において、ルーターについてどのような結論を導き出せますか？

A. ルーター 100.64.3.1 は、ローカル ルーターとの 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. ローカルルーターの受信ルートマップが、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. 表示されているすべてのネイバーは、ローカルルーター上の単一のBGP設定の一部であり、ネイバー範囲は4に設定されています。

D. ピア10.127.0.75とのBGPセッションが確立しました。

正解: **D** (コメントを発表する)

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。Fortinet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「アイドル」、「アクティブ」、「接続中」ではなく、「確立済み」、「稼働中」、または関連するカウンタ（送受信メッセージ数や稼働時間など）が表示されている場合、セッションは正常に動作していることを示します。このシナリオでは、ピア10.127.0.75のみが、稼働中の確立済みセッションを示す肯定的な表示を示しています。ネイバー範囲の設定、ASの不一致、ルートマップによるプレフィックスのブロックなど、その他のオプションは、単純なBGPセッション状態のデバッグで提供される証拠ではサポートされておらず、出力にはローカルまたはリモートASの問題に関連するエラーも表示されません。

正しい解釈は、FortinetのBGPトラブルシューティングガイドに記載されており、デバッグ出力とサマリー出力におけるセッションステータスとネイバー状態の読み方が説明されています。

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: **2**

デバッグ時に iprope_in check () check failed, drop が表示される 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で許可されていないため破棄されました。
B. 送信元への経路がないため、パケットは破棄されました。
C. 信頼済みホストリストの設定ミスにより、パケットが破棄されました。
D. FortiGateで要求されたサービスが有効になっていないため、パケットは破棄されました。
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、特にローカル受信ポリシーチェックの失敗を示します。「iprope」(IPルーティングポリシー適用)エンジンはポリシー検索を処理します。「in_check」という接尾辞は、この決定がFortiGateを通過するトラフィックではなく、FortiGate自体宛てのトラフィック(ローカル受信トラフィック)に関するものである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、パケットは破棄されました。
* 説明: これは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(HTTPSまたはSSHリクエストなど)が到着すると、カーネルはインターフェース設定でその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(set allowaccess)。サービスが有効になっていない場合(例えば、PINGアクセスが無効になっているインターフェースにPingしようとする場合)、iprope_in_check関数が失敗し、パケットは即座に破棄されます。
* C. 信頼済みホストリストの設定が誤っているため、パケットが破棄されました。
* 説明: インターフェースでサービス (HTTPS など) が有効になっている場合でも、FortiGate は管理者設定を確認します。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 アドレスが許可されたリストと比較されます。IP アドレスがリストにない場合、ローカル受信ポリシーチェック (iprope_in_check) が失敗し、管理プレーンを保護するためにパケットが破棄されます。
他の選択肢が間違っている理由:
* A: 標準ファイアウォールポリシーによってトラフィックが破棄された場合(デバイスを介してあるインターフェースから別のインターフェースへトラフィックが通過する場合)、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」と表示されます。これは通常、_in_check ではなく、フォワードチェック(iprope_fwd_check など)です。
* B: ソースへのルートがない場合、エラーは逆パス転送 (RPF) の失敗です。デバッグ フローでは、これを「逆パス チェック失敗、破棄」として明示的にログに記録します。
参照:
FortiGateトラブルシューティングガイド(デバッグフロー):「iprope_in_check()チェックが失敗したというメッセージは、パケットがローカル受信ポリシーによって拒否されたことを示しています。これは、FortiGate宛てのトラフィックがallowaccess設定で許可されていない場合、または信頼済みホスト設定でブロックされている場合に発生します。」

質問: 3
管理者は、内蔵のスニファを使用して、2台のFotiGateデバイス間の暗号化されたフェーズ2トラフィックをキャプチャしたいと考えています。
管理者が、両方のFortiGateデバイス間にNATデバイスが存在しないことを知っている場合、管理者はどのコマンドを実行すべきでしょうか?
A. 診断スニファパケット任意の「udpポート4500」
B. 診断スニファパケット「ip proto 50」
C. スニファパケットを診断して「ah」を検出します
D. 診断スニファパケット任意の「udpポート500」
正解: (正解を表示します)
2台のFortiGateデバイス間で暗号化されたIPsecフェーズ2(ESP)トラフィックをキャプチャするには、適切なプロトコルフィルタとしてip proto 50を使用します。Fortinetの公式スニッフィングおよびデバッグに関するドキュメントによると、ESP(Encapsulating Security Payload)は暗号化されたフェーズ2ペイロード転送に使用され、常にIPプロトコル番号50を使用します。コマンドdiagnose sniffer packet any 'ip proto 50'を実行すると、デバイスから発信されたかデバイスを通過したかにかかわらず、暗号化されたトラフィックを表すESPパケットのみがキャプチャされます。
FortiGate間にNATデバイスがない場合、ESPはUDPでカプセル化されません(したがって、UDPポート4500では使用されません。NAT-Tが必要な場合はパケットはUDPでカプセル化されますが、このシナリオではNATは使用されていないことが明示的に示されています)。UDPポート500はIKE制御(ネゴシエーション)トラフィック用であり、AH(認証ヘッダー、ipプロトコル51)はESPを使用した標準IPsecフェーズ2の暗号化には使用されません。
これは、Fortinetが提供するVPNおよびトラフィック分析に関する公式CLIリファレンスと一致します。
**
参考文献:

FortiOS CLI リファレンス: スニファパケット、ESP、IP プロトコル番号の診断 FortiGate VPN 管理ガイド: IPsec トラフィックのキャプチャと分析

質問: 4
IKEv2では、どの交換によって最初のCHILD_SAが確立されますか？
A. IKE_SA_INIT
B. 情報提供
C. CREATE_CHILD_SA
D. IKE_Auth
正解: **(**正解を表示します**)**
RFC 7296 (IKEv2) および Fortinet の公式ドキュメントによると、IKE_SA_INIT 交換は、暗号化パラメータのネゴシエーション、初期 Diffie-Hellman 交換の実行、および DoS 保護のための Cookie チャレンジ メカニズムの実装を担当します。応答側が 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。イニシエータは、次のリクエストで Cookie を返すことで、主張する IP アドレスに実際に存在することを証明し、リソース枯渇攻撃を軽減します。
この2段階のやり取りにより、応答側はアドレスの証明が成功した後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ます。Fortinetのドキュメントによると、このプロセスはIKE_SA_INITフェーズでのみ発生し、後続のIKE_AuthやCHILD_SAのやり取りでは発生しません。
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: 5
展示資料を参照してください。

Debug output

```
FGT # diagnose debug application ike -1

FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b0b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B708100050 19E253B0B0000006CE3C6FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF68F6A13167A172
26398E                  85 1BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB0000002000000001011 08D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000010 1108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B8204D090A367D8DDDB20E5812CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:b1dd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E3819655C641FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD0000002000000001011 08D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B0000002000000001011 08D293CDB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A09398EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB96B354FF46B84E6A79622FC1D44BC7F964986AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 01A44559000000200000000101 108D283CDB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A83380C0000020000000010 1108D2930DB9994E7E8547D50F9D18113B6CA99000000002
ike 0:VPN_0:24319: out C4906BDD8812D02AE16728D0E893431344D7BC31E9323A2C56E27DB43B747870805D7954558993B25BC43118695BEA47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

デバッグ出力に示されているように、IPsec VPNトンネルが切断されています。

デバッグ出力を分析すると、トンネルがダウンする原因は何だと考えられますか？
A. デッドピア検出が確認パケットを受信していません。
B. 再鍵交換交渉中にトンネルが切断されます。
C. フェーズ2は低下するが、フェーズ1は上昇する。
D. タイマーが切れるとトンネルが落下します。
正解: (正解を表示します)

質問: **6**
証拠資料 1。

```
config system global
    set snat-route-change disable
end
-----------------
config 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
end
```

証拠資料 2。

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= 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=log may_dirty npu f00
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=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

添付資料を参照してください。資料には、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セッション情報の一部が示されています。
管理者は、2つのサービスプロバイダ接続間でセッションのフェイルオーバーが発生しないようにしたいと考えている。
管理者は、既存のセッションが直ちに別のインターフェースを使用するように強制するために、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. port1 の静的ルートの優先度を 11 に変更します。
B. port2 の静的ルートの優先度を 5 に変更します。
C. unset snat-route-change を設定して、デフォルト設定に戻します。
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: 7
展示資料を参照してください。
BGOデバッグコマンドの出力結果を示します。

```
# 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
```

ローカルのFortiGateが近隣のFortiGate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. ローカルルーターはルーター 10.125.0.60 からのキープアライブメッセージを待っています。
B. 3 つの近隣ノードのいずれも、ローカル ルーターとの TCP 3 ウェイ ハンドシェイクを正常に確立できませんでした。
C. ルーター 100.64.3.1 は、ローカル ルーターからの OPEN メッセージを待機しています。
D. ルーター 10.127.0.75 の RIB-OUT 設定により、ローカル ルーターへのルートのアドバタイズが防止されます。
正解: (正解を表示します)
プレフィックスが欠落している理由を特定するには、get router info bgp summary 表示の State/PfxRcd 列と Up/Down 列を解釈する必要があります。
近隣の状況を分析する:
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。
隣接ルーター 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。ルーターはTCP接続の開始を積極的に試みています。
隣人 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）状態あることを示しています。
状態/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、ネイバーからルートが送信されていません。
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、このネイバーにとって接続性やハンドシェイク (オプション A、B、C) は問題ではありません。
状態が「Up」であるにもかかわらず、プレフィックスが0個しか送信されていないという事実は、ネイバーがローカルのFortiGateに送信する前に自身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、これが隣接ルーター（ルーター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）設定の問題であり、ルーターがルートをアドバタイズできないことを正しく特定しています。
参照：
FortiGate Security 7.6 学習ガイド（BGP）：「BGPサマリーにおいて、State/PfxRcdに数値（例0）が表示されている場合、セッションは確立されています。値が0ということは、ピアリングは確立されているものの、ルートが受信されていないことを意味します。これは多くの場合、リモートピアのルートマップまたはプレフィックスリストによるフィルタリングが原因です。」

質問: **8**
デバッグコマンドの出力結果を示す図を参照してください。

出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. 近隣のルーターの1つはルーターIDが0.0.0.4です。

B. インターレースはOSPFバックボーン領域の一部です。

C. vorz4ネットワークセグメントには合計5台のOSPFルーターが接続されています。

D. ポート4に接続されているネットワークで、2台のOSPFルーターがダウンしています。

正解: **(**正解を表示します**)**

質問: **9**
添付の図を参照してください。この図は、get router info routing-table database コマンドの出力の一部を示しています。

管理者は、ポート3に対してデフォルトの静的ルートを設定し、距離を50、優先度を0に設定したいと考えています。
port3のデフォルトスタティックルートが作成された後、port1とport2のデフォルトスタティックルートはどうなりますか？

A. port1 のデフォルト静的ルートが FIB に注入されます。

B. port2 のデフォルト静的ルートが転送情報ベース (FIB) に挿入されます。

C. 出力に表示されている2つのデフォルトの静的ルートは両方ともFIBに注入されます。

D. 出力に示されているどちらの経路も FIB には注入されません。

正解: **(**正解を表示します**)**

質問: **10**
デバッグ時に iprope_in check () check failed, drop が表示される 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で許可されていないため破棄されました。
B. 送信元への経路がないため、パケットは破棄されました。
C. 信頼済みホストリストの設定ミスにより、パケットが破棄されました。
D. FortiGateで要求されたサービスが有効になっていないため、パケットは破棄されました。
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、特にローカル受信ポリシーチェックの失敗を示します。「iprope」（IPルーティングポリシー適用）エンジンはポリシー検索を処理します。「in_check」という接尾辞は、この決定がFortiGateを通過するトラフィックではなく、FortiGate自体宛てのトラフィック（ローカル受信トラフィック）に関するものである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、パケットは破棄されました。
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（HTTPSやSSHリクエストなど）が到着すると、カーネルはインターフェース設定でそのサービスが有効になっているかどうか（set allowaccess）を確認します。サービスが有効になっていない場合（例えば、PINGアクセスが無効になっているインターフェースにPingを試みた場合）、iprope_in_check関数が失敗し、パケットは即座に破棄されます。
C) 信頼済みホストリストの設定が誤っているため、パケットが破棄されました。
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は管理者設定を確認します。
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アドレスが許可されたリストと比較されます。IPアドレスがリストにない場合、ローカル受信ポリシーチェック（iprope_in_check）が失敗し、管理プレーンを保護するためにパケットは破棄されます。
他の選択肢が間違っている理由：
A: 標準ファイアウォールポリシーによってトラフィックが破棄された場合（デバイスを介してあるインターフェースから別のインターフェースへトラフィックが通過する場合）、デバッグメッセージには通常、「ポリシー x により拒否されました」または「一致するポリシーがありません」と表示されます。これは通常、_in_check ではなく、フォワードチェック（iprope_fwd_check など）です。
B: ソースへの経路が存在しない場合、エラーは逆パス転送（RPF）の失敗です。デバッグフローでは、このエラーが「逆パスチェック失敗、破棄」として明示的にログに記録されます。
参照：
FortiGateトラブルシューティングガイド（デバッグフロー）：「iprope_in_check()チェックが失敗したというメッセージは、パケットがローカル受信ポリシーによって拒否されたことを示しています。これは、FortiGate宛てのトラフィックがallowaccess設定で許可されていない場合、または信頼済みホスト設定でブロックされている場合に発生します。」

質問: **11**
展示資料を参照してください。

Diagnose output

```
# diagnose vpn tunnel list name 'VPN'

list ipsec tunnel by names in vd 0

------------------------------------------------------

name=VPN ver=1 serial=8 172.16.50.251:4500->168.138.64.200:4500 tun_id=168.138.64.200 tun_id6=::168.138.64.200 dst_mtu=0 dpd-
link=on weight=1

bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/544 options[0220]=frag-rfc run_state=0 role=primary accept_traffic=1
overlay_id=0


proxyid_num=1 child_num=0 refcnt=6 ilast=59 olast=18 ad=/0

stat: rxp=0 txp=0 rxb=0 txb=0

dpd: mode=on-idle on=1 idle=20000ms retry=3 count=2 seqno=14

natt: mode=keepalive draft=32 interval=10 remote_port=4500

fec: egress=0 ingress=0

proxyid=VPN proto=0 sa=0 ref=1 serial=1

src: 0:0.0.0.0-255.255.255.255:0

dst: 0:0.0.0.0-255.255.255.255:0

run_tally=0
```


コマンド diagnose vpn tunnels liar の出力結果を以下に示します。
トンネルの現状を正確に表しているのは、次のうちどれですか？ 2つ選択してください。）
A. フェーズ2が終了しました
B. フェーズ1は終了しました。
C. 現在、トンネル内を通行する車両はありません。
D. フェーズ1とフェーズ2の両方の交渉が成功裏に完了しました。
正解: (正解を表示します)
Fortinet FCSS - Network Security 7.6 のドキュメントと VPN トンネルの図の分析に基づき、検証済みの回答を以下に示します。

質問: **12**
メモリ負荷のためにFortiGateがメモリ節約モードに入った場合、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はメモリをクリアし、完全な動作を復元するために自動的に再起動します。
B. FortiGateは、フローベースの検査など、メモリ負荷の少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対策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、すべての新規セッションの破棄を開始します。
正解: (正解を表示します)
FortiGateがメモリ負荷の高さ（具体的にはメモリ使用率が95%に達して極限しきい値に達した場合、またはプロキシトラフィックで赤色しきい値に達した場合）によりコンサーブモードに入ると、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、すべての新規セッションの切断を開始します。
* 極限メモリ節約モード（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するよう動作します。そのため、検査の種類に関係なく、すべての新規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規セッション（これらは最も多くのメモリを消費するため）を意図的に破棄しますが、フローベースのトラフィックは多くの場合引き続き許可します。
* 提供されている選択肢の中で、「新しいセッションを破棄する」は、メモリ使用量の増加を阻止するためにFortiOSが採用する唯一の標準的な保護メカニズムです。
他の選択肢が間違っている理由：

* A: FortiGateは、省電力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復旧を試みます。（再起動は最終手段であり、設定可能な動作ではありません。）
* 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、ログ記録やウイルス対策などの「重要でないプロセス」を恣意的に停止することはありません。ログ記録は監査証跡にとって不可欠です。av-failopen を設定することでスキャンをバイパスできますが、システムは通常、エンジン自体を停止するのではなく、「フェイルクローズ」（トラフィックの破棄）をデフォルトとして選択します。
参照：
FortiGate Security 7.6 学習ガイド（診断とリソース使用状況）：「メモリ使用率が極端なしきい値（95%）に達すると、メモリ枯渇を防ぐためにすべての新規セッションが破棄されます。」

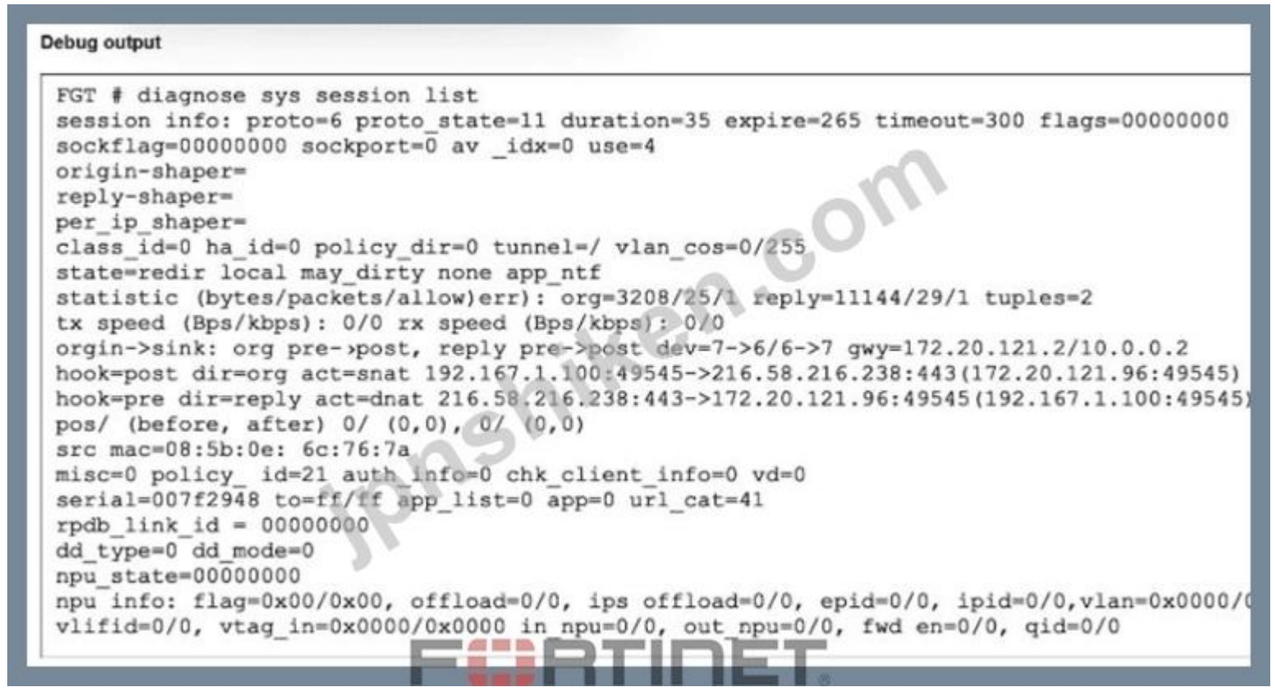
質問: **13**
展示資料を参照してください。


```
# get router info bgp summary

VRF 0 BGP router identifier 172.16.23.58, local AS number 65100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.23.153   4      65100     218     3220        0    0    0 never     Connect

Total number of neighbors 1
```


BGPデバッグコマンドの出力結果を示します。
ローカルルーター（IPアドレス172.16.23.58）が、唯一の隣接ルーターとの隣接関係を確立できないのはなぜですか？
A. 隣接ルーターに到達できなくなっています。これは、受信メッセージ数と送信メッセージ数の比率が低いことから明らかです。
B. ローカルルーターは、ネイバーからOPENメッセージを受信していません。
C. ローカルルーターはネイバーからSYN/ACKパケットを受信していません。
D. BGPネイバーへのアクティブなルートがありません。
正解: (正解を表示します)
正解はCです。
この図では、State/PfxRcd 列にネイバーの状態が Connect と表示されています。学習ガイドでは、BGP の状態について以下のように説明しています。
「接続：3者間TCP接続が正常に確立されるまで待機中」
「OpenSent: ピアからのOPENメッセージを待っています」
「確立済み：ピア間でOPENメッセージとキープアライブメッセージの交換が成功しました」ルーターがまだConnect状態であるため、TCPの3ウェイハンドシェイクは完了していません。実際には、ローカルルーターはTCP SYNを送信しましたが、ハンドシェイクを完了するために必要なSYN/ACKを正常に受信していません。そのため、Cが正解です。
他の選択肢が間違っている理由：
A は、メッセージ カウンターだけではネイバーに到達できないことを証明できないため、間違っています。学習ガイドでは、State/PfxRcd フィールドはセッションが確立されていないときの BGP 状態を示し、ここではその状態は具体的に Connect であると説明されています。B は、OPEN メッセージの待機は Connect ではなく OpenSent で行われるため、間違っています。D はこの出力に対する最良の答えではありません。学習ガイドでは、表示される状態をプロトコル フェーズに直接関連付けています。Connect は、デバイスがまだ正常な TCP ハンドシェイクを待機していることを意味します。したがって、検証済みの答えは C です。

質問: **14**

展示資料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、Iwoが述べた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. 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を行い、正しいポリシーマッチングができるようにしました。

C. FortiGate がセッションを開始したか、FortiGate でセッションが終了したかのいずれかです。

D. FortiGate はこのセッションを検査せずに転送しました。

正解: **(**正解を表示します**)**

セッション出力には以下のフラグが含まれます。

state=redir local may_dirty ...

npu_state=00000000

オフロード=0/0

7.6の学習ガイドでは、これらのフラグについて直接説明しています。

local = "セッションはローカルスタックとの間で行われます"

redir = "セッションはアプリケーション層プロキシによって処理されています"

may_dirty = "セッションはファイアウォールポリシーによって許可されています"

これにより、C が正解となります。ローカル フラグは、セッションが FortiGate から開始されるか FortiGate で終了することを意味するからです。FortiOS 管理ガイドには、同じ意味が記載されています。 ⁋セッションはローカル スタックから開始されるか、ローカル スタック宛てです。」これにより、A も正解となります。redir フラグは、セッションがアプリケーション レイヤー プロキシによって処理されることを意味します。FortiOS ドキュメントでは、プロキシ ベースの検査は FortiGate でトラフィックをバッファリングしてそこで検査し、プロキシ ベースの処理は CPU とメモリを大量に消費すると説明されています。セッションには NPU オフロードも表示されていないため (npu_state=00000000、offload=0/0)、このトラフィックは NPU ではなくソフトウェア/CPU で処理されています。

他の選択肢が間違っている理由：

B は、redir フラグによってセッションが検査なしで通過していないことが証明されるため誤りです。アプリケーション層プロキシによって処理されています。D は、このセッションに認証フラグがないため誤りです。Fortinet のキャプティブ ポータル/認証関連セッションの例では、セッションの状態に auth または authed フラグが含まれています。学習ガイドには、 認証されたユーザーからのトラ

フィックのセッションには、authed フラグが含まれます」と記載されています。この図には auth または authed が表示されていないため、クライアントが認証のためにキャプティブ ポータルにリダイレクトされたと結論付ける根拠はありません。

質問: **15**
図を参照してください。この図は、コマンド get router info bgp neighbors 100.64.2.254 advertised-routes の出力を示しています。

```
# 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
```

この出力からどのような結論が得られますか？
A. BGPネイバーが10.20.30.40/24ネットワークをローカルルーターにアドバタイズしています。
B. 隣接ルーターのIDは100.64.2.254です。
C. 2 つの BGP 参加者の BGP 状態は OpenConfirm です。
D. ローカルルーターは、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。
正解: **(**正解を表示します**)**

質問: **16**
FSSOのリアルタイムデバッグを使用して特定できる、FortiGateとコレクターエージェント間の接続に関する一般的な問題のうち、3つを選択してください。
A. SSL 経由の FSSO に使用されている SSL 証明書の有効期限が切れています。
B. 接続が拒否されました。TCPポートの不一致が考えられます。
C. FortiGate がコレクターエージェントの IP アドレスに到達できません。
D. プロ共有キーが一致しません
E. グループフィルターが一致しません。
正解: **B,C,D (**コメントを発表する**)**
diagnose debug authd fsso server コマンドは、FortiGate と FSSO コレクターエージェント間の通信をトラブルシューティングするための主要なツールです。このデバッグ出力には、接続の状態と障害の原因が表示されます。このデバッグで特定される最も一般的な接続の問題は次の 3 つです。
* FortiGate がコレクターエージェントの IP アドレスに到達できません (オプション C): レイヤ 3 接続が欠落している場合、デバッグには接続タイムアウトまたは「ホストに到達できません」エラーが表示されます。
* 接続が拒否されました / ポートの不一致 (オプション B): FortiGate が IP アドレスに到達できるものの、コレクター エージェントが指定されたポート (デフォルトは 8000) でリッスンしていない場合、デバッグログに「接続が拒否されました」と表示されます。これは、FortiGate で設定されているポートがエージェントのリッスン ポートと一致しない場合によく発生します。
* 事前共有キーが一致しません（オプション D）IP とポートが正しい場合、次のステップは認証です。FortiGate で設定されているパスワードがコレクターエージェントのパスワードと一致しない場合、デバッグログにはハンドシェイク中に「認証失敗」または「パスワード不一致」エラーが明示的に表示されます。

その他のオプションに関する注記：オプションA（SSL）は、基本的な接続/認証の不一致よりも発生頻度が低い。オプションE（グループフィルタ）は、接続確立後に実行されるユーザー処理ロジックに関連する。
参照：
FortiGate Security 7.6 学習ガイド（FSSO トラブルシューティング）：FSSO のトラブルシューティング...接続（IP/ポート）と認証（パスワード）を確認します。」

質問: **17**
ポリシールーティングテーブルのエントリの出力結果を示す図を参照してください。

```
id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
```

出力結果はどのタイプの政策ルートを示していますか？
A. ISDBルート
B. 通常の政策ルート
C. FIB内のアクティブな静的ルートに関連付けられた、通常のポリシールート
D. SD-WANルール
正解: **A (**コメントを発表する**)**
問4の図はポリシー経路テーブルのエントリを示しており、主要なフィールドは以下のとおりです。
* インターネットサービス(1) : Fortinet-FortiGuard(1245324,0.0.0.0,0.0.0.0)
Fortinet の公式ドキュメントによると、ポリシー ルートがインターネット サービス データベース (ISDB) エントリに基づいている場合、ルート エントリには「インターネット サービス」が明示的に記載され、参照されているサービス (この例では Fortinet-FortiGuard) が示されます。これは、ISDB シグネチャを参照せずに送信元、宛先、およびサービスのワイルド カードで定義される通常のポリシー ルートとは根本的に異なります。通常のポリシー ルートの出力には、「インターネット サービス」という行は含まれません。ISDB を使用するポリシー ルートを使用すると、宛先 IP が動的であっても、トラフィック パターン認識に基づいて、FortiGate は特定のよく知られたサービス (FortiGuard、Google、Microsoft など) のトラフィックをルーティングできます。マッチングとルート選択は ISDB タグに従い、静的ポリシー ルートまたは通常のポリシー ルートと共存できます。
したがって、このエントリは、FortiOSのポリシールーティングに関するドキュメントおよびISDB構成リファレンスで説明されているとおり、正しくかつ一意のISDBルートです。
参考文献：
FortiOS 管理ガイド: ポリシールーティング、ISDB 統合、ルーティングテーブルエントリの解釈、Fortinet のドキュメントにおける ISDB ベースのルーティングと公式 CLI 出力

質問: **18**
展示する。

添付の図を参照してください。この図には、get system ha status コマンドの出力結果が示されています。
NGFW-1とNGFW-2は1週間前から稼働している。
出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. この時にプライマリ FortiGate の設定変更が行われた場合、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 デバイスが自身をプライマリとして選出します。
C. FGVM...649 が再起動された場合、FGVM...650 がプライマリとなり、FGVM...649 がクラスタに再参加した後もその役割を維持します。
D. 何も操作を行わない場合、現在の同期状態によりプライマリ FortiGate はクラスタから離脱します。
正解: **(**正解を表示します**)**
FortiGate HAのトラブルシューティングと同期に関するガイド
Fortinet 管理者ガイド :HA プライマリ ロールの保持、同期状態がずれたことによるクラスタの分割

質問: **19**
管理者は、内蔵のスニファを使用して、2台のFotiGateデバイス間の暗号化されたフェーズ2トラフィックをキャプチャしたいと考えています。
管理者が、両方のFortiGateデバイス間にNATデバイスが存在しないことを知っている場合、管理者はどのコマンドを実行すべきでしょうか？
A. 診断スニファパケット任意の「udpポート500」
B. 診断スニファパケット「ip proto 50」
C. 診断スニファパケット任意の「udpポート4500」
D. スニファパケットを診断して「esp」を検出します
正解: **(**正解を表示します**)**

2台のFortiGateデバイス間で暗号化されたIPsecフェーズ2（ESP）トラフィックをキャプチャするには、適切なプロトコルフィルタとしてip proto 50を使用します。Fortinetの公式スニッフィングおよびデバッグに関するドキュメントによると、ESP（Encapsulating Security Payload）は暗号化されたフェーズ2ペイロード転送に使用され、常にIPプロトコル番号50を使用します。コマンドdiagnose sniffer packet any 'ip proto 50'を実行すると、デバイスから発信されたかデバイスを通過したかにかかわらず、暗号化されたトラフィックを表すESPパケットのみがキャプチャされます。
FortiGate間にNATデバイスがない場合、ESPはUDPでカプセル化されません（したがって、UDPポート4500では使用されません。NAT-Tが必要な場合はパケットはUDPでカプセル化されますが、このシナリオではNATは使用されていないことが明示的に示されています）。UDPポート500はIKE制御（ネゴシエーション）トラフィック用であり、AH（認証ヘッダー、ipプロトコル51）はESPを使用した標準IPsecフェーズ2の暗号化には使用されません。
これは、Fortinetが提供するVPNおよびトラフィック分析に関する公式CLIリファレンスと一致します。
**
参考文献：
FortiOS CLI リファレンス: スニファパケット、ESP、IP プロトコル番号の診断 FortiGate VPN 管理ガイド: IPsec トラフィックのキャプチャと分析

質問: **20**
展示資料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
```

すべての経路が同じ距離に設定されている場合、トラフィックはどの経路を通って100.65.0.0/24ネットワークに到達するでしょうか？
A. BGPルート
B. 政策ルート
C. 静的ルート
D. OS PFルート
正解: **(**正解を表示します**)**

トラフィックがたどる経路を決定するには、FortiGate のルート検索優先順位 (パケット処理フロー) と、図 「ルーティング優先順位の分析」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、パケットが到着したとき（既存のセッションの一部ではない場合）、FortiGateは特定の順序で経路検索を実行します。
ポリシールート（config router policy または diagnose firewall proute list）で設定します。これらは最初にチェックされます。パケットが条件（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、ポリシールートが即座に使用されます。
FIB（転送情報ベース）ポリシー ルートに一致するものがない場合、デバイスは標準ルーティング テーブル（静的、接続済み、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 (質問にあるネットワークと一致します)。
動作: oif=6(ポート4)経由でゲートウェイ10.0.4.253にトラフィックを転送します。
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、複数のルートが表示されます。
100.65.0.0/24 (スタティック、OSPF、BGP) 全て距離10。現在、FIBではスタティックルート(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の指示に従ってトラフィックを転送します。ポリシールートの条件（入力ポート3）に一致するトラフィックに対しては、ルーティングテーブルに表示されるスタティックルート、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: 21
展示資料を参照してください。

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以下に示します。この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. 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 イベントを検出します。
C. FortiGate は、ユーザーがログアウトしたかどうかを確認するために、ワークステーションを頻繁にポーリングします。
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。
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」を実行すると、FortiGate シングルサインオンデーモンの内部処理が明らかになります。
* オプション D (エージェントレス ポーリング): 出力には event_id=4768 と表示されます。イベント ID 4768 (Kerberos TGT リクエスト) は Windows イベント ログのエントリです。一般的なログオン通知ではなく、fssod デバッグに特定のイベント ID が存在することは、システムがドメイン コントローラーからセキュリティ イベント ログを読み取っている (ポーリングしている) ことを示しています。これは、FortiGate またはコレクターがログを収集するエージェントレス ポーリング モード (またはコレクター エージェント ポーリング モード) の特徴です。これに対し、DC エージェント モードではログオン呼び出しを直接インターセプトし、通常はワークステーション名を含むより完全な情報を提供します。
* オプション A (検証): 重要な点として、出力に workstation=, と表示され、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) には、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なため、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、DCエージェントがワークステーション名を確実に取得するため誤りです。オプションCは、システムが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誤りです。

質問: **22**
展示資料を参照してください。

Diagnose output

```
#diagnose debug application ike -1
#diagnose debug enable
.....
ike V-root:0:VPN_IKEv2:29: received create-child request
ike V-root:0:VPN_IKEv2:29: responder received CREATE_CHILD exchange
ike V-root:0:VPN_IKEv2:29: responder creating new child
ike V-root:0:VPN_IKEv2:29:10: peer proposal:
ike V-root:0:VPN_IKEv2:29:10: TSi_0 0:10.1.2.0-10.1.2.255:0
ike V-root:0:VPN_IKEv2:29:10: TSr_0 0:10.1.1.0-10.1.1.255:0
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: comparing selectors
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: matched by rfc-rule-2
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: phase2 matched by subset
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: accepted proposal:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: TSi_0 0:10.1.2.0-10.1.2.255:0
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: TSr_0 0:10.1.1.0-10.1.1.255:0
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: autokey
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: incoming child SA proposal:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: proposal id = 1:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:   protocol = ESP:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:      encapsulation = TUNNEL
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ENCR, val=3DES_CBC
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=INTEGR, val=SHA256
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=DH_GROUP, val=MODP2048
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=DH_GROUP, val=MODP1536
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ESN, val=NO
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: my proposal:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: proposal id = 1:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:   protocol = ESP:
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:      encapsulation = TUNNEL
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ENCR, val=3DES_CBC
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=INTEGR, val=SHA256
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=DH_GROUP, val=MODP3072
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ESN, val=NO
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: lifetime=300
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: no proposal chosen
ike V-root:Negotiate SA Error: [1401]
ike V-root:0:VPN_IKEv2:29:VPN_IKEv2:10: responder preparing CREATE_CHILD message
ike 0:VPN_IKEv2:29: enc 0000000800000000E0706050403020100
ike 0:VPN_IKEv2:29: out
```

IKEv2を使用したIPsec VPNトンネルは正常に確立されましたが、トンネルの鍵交換が行われるとトンネルが切断されます。
IKEのデバッグコマンドが有効になっており、図にはトンネルの起動を試みた際のデバッグIKEの出力の一部が示されています。
トンネルが閉鎖されている原因は何ですか？

A. ディフィー・ヘルマン不一致
B. UDPポート500のトラフィックがブロックされました
C. 第1段階交渉におけるミスマッチ
D. 第2段階交渉における不一致

正解: **(正解を表示します)**
障害の原因を特定するには、添付資料（image_ad3dc6.jpg）に示されている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、レスポンダーが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の鍵を再生成するために使用されます。
トンネルが以前に「正常に確立された」という事実は、初期IKE SA（フェーズ1）が安定していることを意味し、このエラーは特に鍵交換イベント中に発生しており、そのイベントには多くの場合、完全前方秘匿性（PFS）が関係しています。
提案内容を分析する（不一致点）：
受信提案（リモートピア）：
リモートピアは、2つのDiffie-Hellmanグループ（type=DH_GROUP、val=MODP2048（グループ14）とtype=DH_GROUP、val=MODP1536（グループ5））を含む提案を送信します。
私の提案（ローカルFortiGate）：
ローカルの FortiGate 設定では、type=DH_GROUP、val=MODP3072 (グループ 15) が想定されます。
交渉結果：
デバッグ出力の最後には、「提案が選択されませんでした」および「SA交渉エラー」が表示されます。
このエラーは、ローカルのFortiGateが、要求するDiffie-Hellmanグループ（グループ15）とピアが提供するDiffie-Hellmanグループ（グループ14または5）の間で共通の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）の作成中に発生した不一致ですが、ログで特定された正確な根本原因は「Diffie-Hellman不一致」（オプションA）です。
他の選択肢が間違っている理由：
B: ログには子作成リクエストが受信されたことが示されており、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できます。
C: 障害は、IKE_SA_INIT または IKE_AUTH (フェーズ 1) の交換ではなく、CREATE_CHILD 交換 (フェーズ 2/鍵の再作成) で発生しています。
D: 不一致はフェーズ2の定義内で発生していますが、DH_GROUP行に表示されてい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のパラメータ…完全前方秘匿性（PFS）が有効になっている場合、Diffie-Hellman鍵交換が再度実行されます。両方のピアはDHグループが一致している必要があります。

質問: **23**
展示資料を参照してください。

Output of `diagnose npu np6 port-list` on FortiGate 2000E

```
Chip    XAUI  Ports    Max    Cross-chip
                        Speed  offloading
------  ----  -------  -----  ----------
np6_1   0     port1    1G     No
        0     port5    1G     No
        0     port9    1G     No
        0     port13   1G     No
        0     port17   1G     No
        0     port21   1G     No

-omitted-
```


FortiGate 2000E 上で diagnose npu up6 port-list コマンドを実行した際の出力の一部を以下に示します。
管理者は、diagnose snifferコマンドを使用してポート1とポート17間のトラフィックを分析することができません。
管理者がトラフィックを表示できるようにするコマンドはどれですか？ 2つ選択してください。）

A.
```
diagnose npu np6 port-list disable 5 17
```

B.
```
config firewall policy
edit 5
set auto-asic-offload disable
end
next
edit 17
set auto-asic-offload disable
end
```

C.
```
diagnose npu np6 fastpath disable 1
```

D.
```
config system npu
set fastpath disable
end
```

正解: (正解を表示します)
管理者は、トラフィックがNPU (NP6)にオフロードされているため、スニファでトラフィックを確認できません。トラフィックを表示するには、オフロードを無効にしてパケットがCPUを通過するようにする必要があります。
* B. config firewall policy ... set auto-asic-offload disable: これは、特定のトラフィックのトラブルシューティングに推奨される方法です。関連するファイアウォール ポリシー (図のポリシー 5 と 17) で ASIC オフロードを無効にすると、トラフィックは CPU に強制的に送られ、スニファで確認できるようになります。

* C. diagnose npu np6 fastpath disable 1: このコマンドは、ポートを処理する特定のNP6プロセッサ（ID 1）の高速パス処理を一時的に無効にします。これにより、そのNPUによって処理されるすべてのトラフィックがCPUに強制的に転送され、スニファがそれをキャプチャできるようになります。
* 不適切なオプション：オプションAは無効な構文を使用しています（port-list disableは有効なコマンドではありません）。オプションD（config system npu）は、詳細なトラブルシューティングのための標準的な方法ではありません。

質問: **24**
リアルタイムOSPFデバッグの出力の一部を示す図を参照してください。

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 0x2f85
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
```

なぜ2台のFortiGateデバイスは隣接関係を確立できないのでしょうか？
A. 隣接関係を確立しようとしている 2 台の FortiGate デバイスは、エリア 0.0.0.0 にあります。
B. HelloパケットはID 0.0.0.112のOSPFルーターから送信されています。
C. FortiGateデバイスのパスワードが一致しません。
D. 一方のFortiGateデバイスは認証を要求するように設定されていますが、もう一方は認証を要求しません。
正解: (正解を表示します)

質問: **25**

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

出力結果から、どのような2つのことが分かりますか？（2つ選択してください。）
A. 設定がバックアップされました
B. 高可用性（HA）フェイルオーバーが発生しました。
C. この試みは失敗に終わった。

D. 自動ステッチテストがログに記録されていません。
正解: **(**正解を表示します**)**
観察結果を判断するには、展示資料に示されている特定のCLI出力を分析する必要があります。
* コマンドと出力の分析：
* コマンド: # 自動化テスト HAFailOver を診断する
* このコマンドは、自動化ステッチ（「HAFailOver」という名前）を手動でトリガーして、その構成とアクションの実行を確認するために使用されます。トリガーイベントをシミュレートして、定義されたアクションを実行します。
* 出力: 自動化テストが失敗しました(1)。stitch:HAFailOver
* 出力には、テストが失敗したことが明示的に示されています。コード（1）は、実行が正常に完了しなかったことを示す一般的なエラーコードです。
* 選択肢を評価する：
* A. 設定はバックアップされました。
* 誤りです。テスト結果が「失敗」であるため、ステッチで定義されたアクション（「HAFailOver」という名前から推測すると、「バックアップ構成」である可能性が高い）は正常に実行されませんでした。
* B. 高可用性（HA）フェイルオーバーが発生しました。
* 誤りです。コマンド「diagnose automation test」はシミュレーションツールです。実際の物理的なHAフェイルオーバーが発生したことを示すものではなく、そのイベントに関連付けられたスクリプトを実行しようとするだけです。
* C. テストは失敗しました。
* 正解です。出力には「自動化テストが失敗しました(1)」と明確に表示されており、これはテストが失敗したことの定義です。
* D. 自動化ステッチテストがログに記録されていません。
* 正解です。Fortinetの自動化トラブルシューティングにおいて、「失敗(1)」の結果は、ステッチが無効になっている場合、またはステッチをトリガーまたは記録するために必要なログ設定が有効になっていない場合に発生することがよくあります。その結果、テスト実行が自動化履歴に適切に記録されないか、または失敗は処理を進めるために必要なログデータが不足していることを意味します。明らかに誤った選択肢AとBを除外すると、Dが2番目に正しい考察となります。
参照：
FortiGate Security 7.6 学習ガイド（セキュリティファブリックと自動化）：「自動化ステッチは、CLI コマンド diagnose automation test <stitch_name> を使用してテストできます。コマンドが「failed」を返した場合、アクションが実行されなかったことを意味します。これは多くの場合、ステッチが無効になっているか、パラメータが無効になっていることが原因です。」

質問: **26**
デバッグコマンドの出力結果を示す図を参照してください。

出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. インターレースはOSPFバックボーン領域の一部です。

B. vorz4ネットワークセグメントには合計5台のOSPFルーターが接続されています。

C. 近隣のルーターの1つはルーターIDが0.0.0.4です。

D. ポート4に接続されているネットワークで、2台のOSPFルーターがダウンしています。

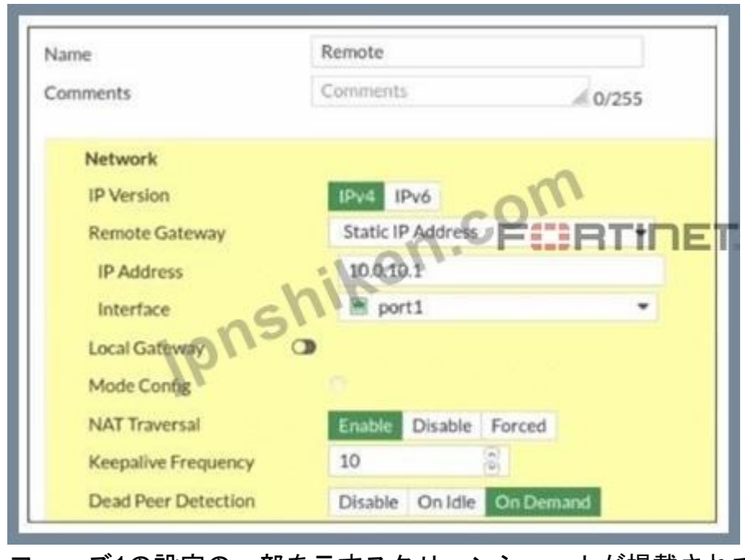
正解: **(**正解を表示します**)**

参考文献：

FortiOS 管理者ガイド :OSPF、デバッグ出力

質問: **27**

展示する。



フェーズ1の設定の一部を示すスクリーンショットが掲載されている資料を参照してください。

VPNが起動していません。この問題を診断するために、管理者はFortiGateのSSHセッションで以下のCLIコマンドを入力します。

```
diagnose vpn ike log-filter dst-addr4 10.0.10.1
diagnose debug application ike -1
```

しかし、IKEのリアルタイムデバッグでは何も出力されません。なぜでしょうか？

A. 管理者は、diagnose debug enable コマンドも実行する必要があります。

B. デバッグではエラーメッセージのみが表示されます。出力がない場合は、フェーズ1とフェーズ2の設定が一致しています。

C. ログフィルタの設定が間違っています。VPNトラフィックはこのフィルタに一致しません。

D. diagnose debug application ike -1 を diagnose debug application ipsec -1 に置き換えます。

正解: **(**正解を表示します**)**

FortiGate デバイスでデバッグ出力を表示するには、アプリケーション固有のデバッグ コマンドとグローバル デバッグ有効化コマンドの両方を必ず実行する必要があります。コマンド diagnose debug application ike -1 は IKE デーモンのデバッグの詳細レベルを設定しますが、単独ではデバッグ出力は表示されません。FortiOS CLI デバッグ マニュアルに記載されているように、コマンド diagnose debug enable を実行すると、コンソールにデバッグ出力が有効になり、以前に設定されたすべてのデバッグ情報が表示されるようになります。これは、VPN のトラブルシューティングにおいて特に重要です。enable コマンドがないと、VPN トラフィックがあっても出力は表示されません。

正しい診断手順は以下のとおりです。

診断デバッグアプリケーション ike -1

診断デバッグ有効化

この手順は、すべてのFortiOS CLIデバッグチュートリアルおよびトラブルシューティングワークフローに記載されています。

参考文献：

FortiOS CLI リファレンス: VPN のデバッグとリアルタイムデバッグ出力

FortiGate VPNトラブルシューティングガイド :デバッグ出力に必要な手順

質問: **28**

IKEv2において、DoS攻撃対策を提供している取引所はどれですか？

A. IKE_Req_INIT

B. IKE_Auth

C. IKE_SA_NIT

D. 子どもの子どもを作成する

正解: **(**正解を表示します**)**

質問: **29**

図を参照してください。図には、ウェブフィルタプロファイルの構成の一部が示されています。

URL www.dropbox.com は、ファイル共有とストレージに分類されます。
ユーザーがwww.dropbox.comにアクセスしようとした場合、FortiGateはどのような動作を実行しますか？
A. FortiGate は無効な URL として接続をブロックします。
B. FortiGuardのカテゴリベースのフィルタ設定に基づいて、FortiGateが接続をブロックします。
C. Webコンテンツフィルタの設定に基づき、www.dropbox.comへのアクセスは除外されます。
D. URLフィルタの設定に基づいて、FortiGateは接続を許可します。
正解: **(**正解を表示します**)**

質問: **30**
展示資料を参照してください。

デフォルト設定を前提とした場合、正しい記述は次のうちどれですか？ (3つ選択してください。)

A. 厳密な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を使用して95.56.234.24へのルートがありません。

C. ユーザーA: 合格。wan1を経由するデフォルトの静的ルートは、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 宛て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 へのルートがありません。

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: **31**

特定のセッションが一時的なものとして分類されるのは、次のうちどの2つの分類表ですか？ (2つ選択してください。)

A. 受信パケットが1つだけのUDPセッション

B. パケットの送受信を伴うUOPセッション

C. SYN ACKを待機しているTCPセッション

D. FIN ACKを待機中のTCPセッション

正解: **A,C (**コメントを発表する**)**

学習ガイドには次のように記載されています。

「FortiGateは、セッションテーブルのエントリがTCPセッションが完全に確立されていない場合（3ウェイハンドシェイクが完了していない場合）、またはUDPセッションでパケットが1つしか受信されていない場合に、そのエントリを一時的なセッションとして分類します。」これは直接的に次のことを証明しています。

Aが正解です。なぜなら、受信したパケットが1つだけのUDPセッションは一時的なものだからです。

Cが正解です。SYN/ACKを待っているTCPセッションは完全に確立されていないため、一時的なものです。学習ガイドのTCP状態表によると、ハンドシェイクはセッションがESTABLISHEDに達したときにのみ完了します。他の選択肢が間違っている理由：Bは誤りです。UDPトラフィックが双方向で確認されると、一時セッションで説明されている「単一パケット受信」の状態ではなくなります。学習ガイドでは、UDPの場合、00は一方向、01は双方向とされています。Dは誤りです。FIN/ACKを待機しているTCPセッションは、確立後すでに終了段階にあり、「完全に確立されていない」段階ではありません。学習ガイドでは、両側がセッションを閉じた後、FortiGateはFIN/ACK後の順不同パケットの状態値5で、セッションを一時的にテーブルに保持できると説明されています。

質問: **32**

添付資料を参照してください。資料には、`diagnose vpn tunnel list` コマンドの出力結果が含まれています。

```
diagnose vpn tunnel list
name=DialUp_0 ver=1 serial=4 10.200.1.1:4500->10.200.3.2:64916 tun_id=10.200.3.2 dst_mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0
parent=DialUp index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=221 txp=0 rxb=35360 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=70
natt: mode=silent draft=32 interval=10 remote_port=64916
proxyid=DialUp proto=0 sa=1 ref=2 serial=3 add-route
  dst: 0:0.0.0.0-255.255.255.255:0
  src: 0:10.0.10.10-10.0.10.10:0
  SA:  ref=3 options=82 type=00 soft=0 mtu=1422 expire=43065/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000079 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=5ed4aafc esp=aes key=16 054852d43abb0e931641b4e88781d9ce
       ah=sha1 key=20 082eafd018bf7d4d7b65d9c5b7448db5cc01e81d
  enc: spi=69d4231e esp=aes key=16 d5a23d09ab4128d094ac172f511f9db
       ah=sha1 key=20 54eac30e29ce711d2ceaab9b0e1[illegible]3605e
  dec:pkts/bytes=120/10080, enc:pkts/bytes=0/0
```

DialUp_0という名前のVPNのESPトラフィックをキャプチャするには、どのコマンドを使用すればよいでしょうか？

A. 診断スニファパケット任意の「port4500」

B. 診断スニファパケット「host 10.0.10.10」

C. 診断スニファパケット「esp」およびホスト10.200.3.2「

D. 診断スニファパケット 'ip proto 50'

正解: (正解を表示します)

質問: **33**

展示資料を参照してください。

```
config system interface
    edit "port1"
        set preserve-session-route enable
    next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=60 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state=log may_dirty npu f00 route_preserve
orgin->sink: org pre->post, reply pre->post dev=7->19/[illegible] gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 [illegible] master=0
```

FortiGateのport1インターフェースの設定と、ICMPトラフィックに関するセッション情報の一部を示します。

このセッションに影響を与えるルーティング変更が発生した場合、セッション情報にはどのような変化が起こりますか？ 2つ選択してください）

A. このセッションはルーティング変更の影響を受けません。ルーティング変更は新規セッションにのみ適用されます。

B. セッションはダーティとしてフラグ付けされますが、ルート検索は実行されません。

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. アクティブなルートがルーティングテーブルから削除されても、セッション情報は変更されません。

正解: (正解を表示します)

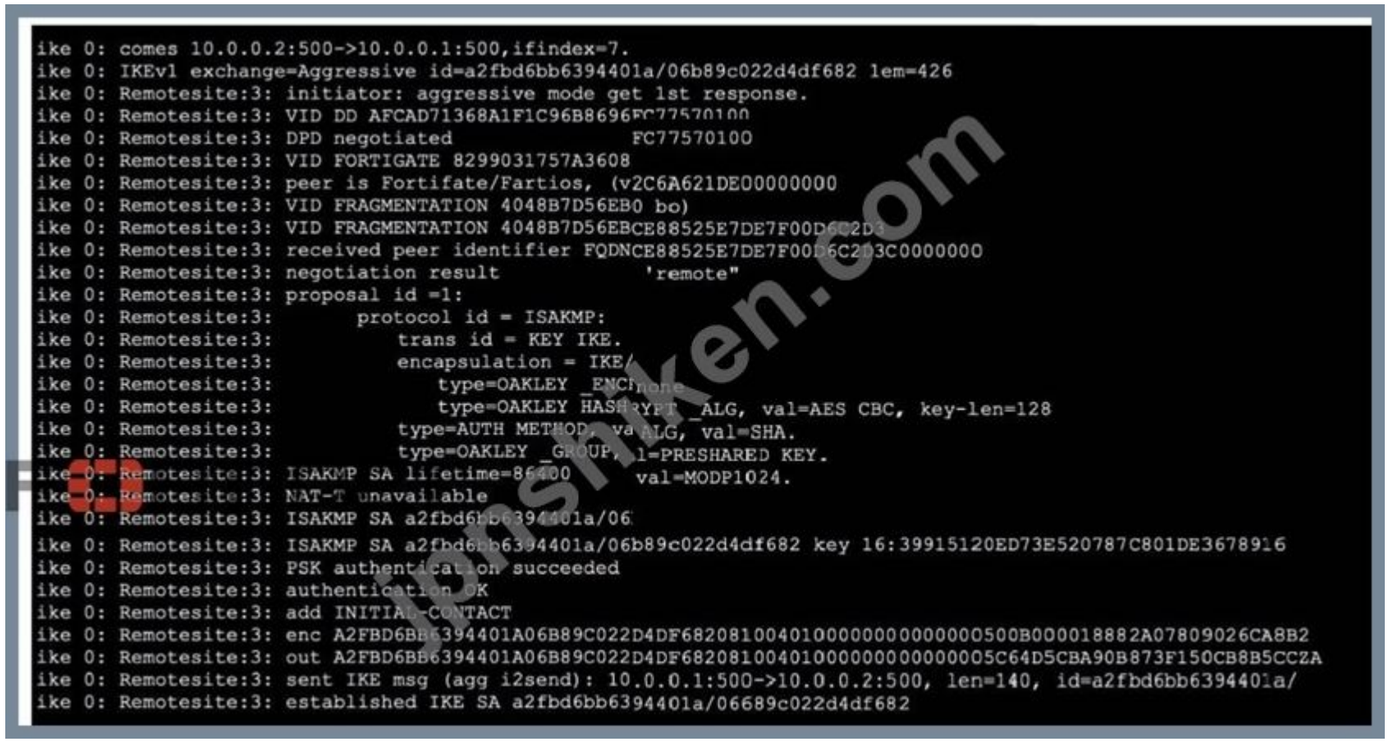
正解はAとCです。
この表示は、ポート1でpreserve-session-routeが有効になっていることを示しています。
設定システムインターフェース
 「ポート1」を編集
set preserve-session-route enable
次
終わり
学習ガイドでは、この設定がもたらす影響について具体的に説明しています。
 「有効化：FortiGateは既存のセッションルーティング情報を永続的にマークし、変更されたルートのみを新しいセッションに適用します」また、次のように記載されています。
 「現在のルートはFIBに存在している必要があります。そうでない場合、FortiGateはセッションをダーティとしてフラグ付けし、再評価します。」そして、同じページではさらに次のように説明しています。
 「この設定を有効にすると、そのインターフェイスを通過するセッションはルーティングの変更の影響を受けることなく通過し続けます。ルーティングの変更は新しいセッションにのみ適用されます。ルートがFIBから削除された場合、FortiGateはセッションをダーティとしてフラグ付けし、ゲートウェイ情報をフラッシュして、セッションを再評価する必要があります。」これは次のことを証明しています。
Aが正解です。preserve-session-routeを有効にすると、既存のセッションは通常保持され、ルーティングの変更は新しいセッションにのみ適用されます。
Cが正解です。現在のルートがFIB/ルーティングテーブルから削除されない限り、セッションは変更されません。削除された場合は、FortiGateがセッションをダーティにして再評価します。
他の選択肢が間違っている理由：
Bは誤りです。アクティブなルートが削除された場合でも、FortiGateは単にセッションをダーティとしてマークしてそこで停止するわけではありません。学習ガイドには 「セッションをダーティとしてフラグ付けし、再評価する」と記載されており、これはルート検索が再度実行されることを意味します。
Dは誤りです。アクティブなルートが削除されると、セッションは変更されます。FortiGateはゲートウェイ情報をフラッシュし、セッションを再評価します。
したがって、検証済みの回答はA、Cです。

質問: **34**
FortiOSカーネルスラブの一部の出力を示す図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
...
```

次の記述のうち、正しいものはどれですか？
A. 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。
B. sctp_session スラブの合計スラブサイズは 0 kB で、ユーザー空間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. ip_session スラブの合計スラブサイズは 3600 kB で、ユーザー空間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: **35**
展示する。



IKEリアルタイムデバッグの出力の一部を含む図を参照してください。

このデバッグ出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. 設定で完全前方秘匿性 (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. これは第2段階の交渉を示しています。

D. イニシエータは、IPsecピアIDとしてremoteを提供しました。

正解: **C,D** (コメントを発表する)

この図から、デバッグ出力がアグレッシブモードでのIKEv1ネゴシエーションを捉えていることがわかります。

Fortinetの公式IPsec VPNトラブルシューティングリソースおよびデバッグガイドに沿って、関連する詳細を詳しく見ていきましょう。

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ています。

10.0.0.2:500->10.0.0.1:500 が、ifindex=7 で発生します。

これは、トラフィックの方向を示しています。リモートIPアドレス（10.0.0.2）のポート500からローカルIPアドレス（10.0.0.1）のポート500へのトラフィックです。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はローカルゲートウェイのIPアドレスです。

オプションDの場合：

次の声明をご覧ください。

交渉結果は「遠い」

そして

ピア識別子FQDNCE88525E7DE7F00D6C2D3C00000000を受信しました

公式デバッグドキュメントによると、ここに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が表示されます。IKE/IPsecネゴシエーションにおいては、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」を指定しています。

AまたはCではない理由：
完全前方秘匿性（PFS）デバッグではフェーズ2での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などへの参照はありません）。そのため、この出力だけではPFSの存在を推測することはできません。
フェーズ2の交渉：ログはIKE（フェーズ1）の交渉と確立に焦点を当てており、フェーズ2のSA交渉と確立を示すESPプロトコル、クイックモード、その他の識別子への言及はありません。
この解釈は、FortiOS 7.6.4 管理ガイドの VPN セクションの説明、および Fortinet のドキュメントに掲載されている公式デバッグコマンドの出力例と一致しています。ローカル アドレスとリモート アドレスを区別する方法、およびピア 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 管理者ガイド：IPsec VPNとVPNのデバッグ
IKEデバッグ出力とピアIDロールの解釈に関するテクニカルサポートリソース

質問: **36**
展示する。

図を参照してください。これは、diagnose hardware aysinfo memory の出力の一部を示しています。
出力に関する記述のうち、正しいものはどれですか？（2つ選択してください。）
A. 641364 kBのメモリが割り当てられているI/Oキャッシュ。
B. 98908 kB のメモリが未使用のままです。
C. ユーザー空間には、システムで使用されていない物理メモリが 708880 kB あります。
D. 非アクティブな見出しの横に表示されている値は、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: **B,D** (コメントを発表する)

質問: **37**
デバッグ出力を示す図を参照してください。

管理者がFSSOをDCエージェントモードで展開しましたが、FortiGate上でFSSOが失敗しています。コレクターエージェントが展開されている場所からFortiGateへのpingは成功しています。
管理者はその後、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。
B. FortiGate は Active Directory サーバー名を解決できません。
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. 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: 38

展示資料を参照してください。

Diagnose output

```
#diagnose debug application ike -1
#diagnose debug enable
.....
ike V=root:0:VPN_IKEv2:29: received create-child request
ike V=root:0:VPN_IKEv2:29: responder received CREATE_CHILD exchange
ike V=root:0:VPN_IKEv2:29: responder creating new child
ike V=root:0:VPN_IKEv2:29:10: peer proposal:
ike V=root:0:VPN_IKEv2:29:10: TSi_0 0:10.1.2.0-10.1.2.255:0
ike V=root:0:VPN_IKEv2:29:10: TSr_0 0:10.1.1.0-10.1.1.255:0
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: comparing selectors
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: matched by rfc-rule-2
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: phase2 matched by subset
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: accepted proposal:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: TSi_0 0:10.1.2.0-10.1.2.255:0
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: TSr_0 0:10.1.1.0-10.1.1.255:0
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: autokey
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: incoming child SA proposal:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: proposal id = 1:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:   protocol = ESP:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:      encapsulation = TUNNEL
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ENCR, val=3DES_CBC
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=INTEGR, val=SHA256
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=DH_GROUP, val=MODP2048
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=DH_GROUP, val=MODP1536
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ESN, val=NO
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: my proposal:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: proposal id = 1:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:   protocol = ESP:
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:      encapsulation = TUNNEL
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ENCR, val=3DES_CBC
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=INTEGR, val=SHA256
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=DH_GROUP, val=MODP3072
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10:         type=ESN, val=NO
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: lifetime=300
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: no proposal chosen
ike V=root:Negotiate SA Error: [1401]
ike V=root:0:VPN_IKEv2:29:VPN_IKEv2:10: responder preparing CREATE_CHILD message
ike 0:VPN_IKEv2:29: enc 0000000800000000E0706050403020107
ike 0:VPN_IKEv2:29: out
```

IKEv2を使用したIPsec VPNトンネルは正常に確立されましたが、トンネルの鍵交換が行われるとトンネルが切断されます。

IKEのデバッグコマンドが有効になっており、図にはトンネルの起動を試みた際のデバッグIKEの出力の一部が示されています。

トンネルが閉鎖されている原因は何ですか？

A. ディフィー・ヘルマン不一致

B. UDPポート500のトラフィックがブロックされました

C. 第1段階交渉におけるミスマッチ

D. 第2段階交渉における不一致

正解: **A** (コメントを発表する)

障害の原因を特定するには、添付資料（image_ad3dc6.jpg）に示されている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、レスポンダーが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の鍵を再生成するために使用されます。

トンネルが以前に「正常に確立された」という事実は、初期IKE SA（フェーズ1）が安定していることを意味し、このエラーは特に鍵交換イベント中に発生しており、そのイベントには多くの場合、完全前方秘匿性（PFS）が関係しています。
提案内容を分析する（不一致点）：
受信提案（リモートピア）：
リモートピアは、2つのDiffie-Hellmanグループ（type=DH_GROUP、val=MODP2048（グループ14）とtype=DH_GROUP、val=MODP1536（グループ5）を含む提案を送信します。
私の提案（ローカルFortiGate）：
ローカルの FortiGate 設定では、type=DH_GROUP、val=MODP3072 (グループ 15) が想定されます。
交渉結果：
デバッグ出力の最後には、「提案が選択されませんでした」および「SA交渉エラー」が表示されます。
このエラーは、ローカルのFortiGateが、要求するDiffie-Hellmanグループ（グループ15）とピアが提供するDiffie-Hellmanグループ（グループ14または5）の間で共通の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）の作成中に発生した不一致ですが、ログで特定された正確な根本原因は「Diffie-Hellman不一致」（オプションA）です。
他の選択肢が間違っている理由：
B: ログには子作成リクエストが受信されたことが示されており、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できます。
C: 障害は、IKE_SA_INIT または IKE_AUTH (フェーズ 1) の交換ではなく、CREATE_CHILD 交換 (フェーズ 2/鍵の再作成) で発生しています。
D: 不一致はフェーズ2の定義内で発生していますが、DH_GROUP行に表示されてい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のパラメータ…完全前方秘匿性（PFS）が有効になっている場合、Diffie-Hellman鍵交換が再度実行されます。両方のピアはDHグループが一致している必要があります。

質問: 39
展示する。

```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
   <2023/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
    FGVM010000077649(updated 4 seconds ago): in-sync
    FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
    FGVM010000077649(updated 4 seconds ago):
        sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
    FGVM010000077650(updated 1 seconds ago):
        sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
    FGVM010000077649(updated 4 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
    FGVM010000077650(updated 1 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary     : NGFW-1          , FGVM010000077649, HA cluster index = 1
Secondary   : NGFW-2          , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

添付の図を参照してください。この図には、get system ha status コマンドの出力結果が示されています。
NGFW-1とNGFW-2は1週間前から稼働している。
出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. この時にプライマリ FortiGate の設定変更が行われた場合、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 デバイスが自身をプライマリとして選出します。
C. FGVM...649 が再起動された場合、FGVM...650 がプライマリとなり、FGVM...649 がクラスタに再参加した後もその役割を維持します。
D. 何も操作を行わない場合、現在の同期状態によりプライマリ FortiGate はクラスタから離脱します。
正解: **B,C** (コメントを発表する)
FortiGate HAのトラブルシューティングと同期に関するガイド
Fortinet 管理者ガイド :HA プライマリ ロールの保持、同期状態がずれたことによるクラスタの分割

質問: **40**
展示資料を参照してください。

```
---omitted---
[ 7608] wksta_check: failed to connect to workstation:10.0.155.23 (10.0.155.23)
[ 7608] wksta_check_wmi: cannot get UserName, error code:0x0
---omitted---
```

コレクターエージェントのログ出力が表示されています。コレクターエージェントは、ワークステーションの状態を 未検証」と表示しています。このメッセージが表示される一般的な原因を2つ挙げてください。2つ選択してください。）
A. ワークステーションが休止状態から復帰しました。
B. ワークステーションのリモートレジストリサービスが実行されていません。
C. ポート139と445へのトラフィックはブロックされています。
D. DNS でワークステーション名を解決できません。
正解: (正解を表示します)
正解はBとCです。
学習ガイドには コレクターエージェントの未確認ステータス」というタイトルのセクションがあり、次のように記載されています。
収集エージェントは、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」というメッセージが表示され、よくある原因として以下のものが挙げられています。
ファイアウォールがポート139と445へのトラフィックをブロックしています」
ワークステーションのリモートレジストリサービスが実行されていません」
ガイドには検証方法も記載されています。
WMIポーリングモードの場合、コレクターエージェントはWMIサービスをチェックします。その他のすべてのモードでは、コレクターエージェントはリモートレジストリサービスを介してHKEY_USERSハイブをチェックします。」ワークステーションがこれらのチェックに応答しない場合、ステータスは未検証になる可能性があります。同じ学習ガイドの追加要件スライドでは、次のことが確認されています。
コレクターエージェントとすべてのワークステーション間で、TCPポート139番と445番を開放する必要があります。」
各ワークステーションでリモートレジストリサービスが稼働している必要があります」
他の選択肢が間違っている理由：
A は、学習ガイドでワークステーションが休止状態から復帰することについて別の問題 IP アドレス変更後にインターネットに接続できない」で言及されており、検証されていない状態の一般的な原因としてではないため、誤りです。D は、DNS 解決の問題も IP アドレス変更シナリオで説明されており、コレクターエージェントが IP アドレス変更後に DNS を使用してワークステーション名を解決するため、このログメッセージに記載されている検証されていない原因とは別であるため、誤りです。したがって、検証済みの回答は B、C です。

質問: **41**
ローカルOSPFルーターがピアとの隣接関係を確立できません。
管理者は、この問題のトラブルシューティングのために、次のうちどれを行うべきですか？ 2つ選択してください。）
A. 両方のピアが同じサブネット内のIPアドレスを持っているかどうかを確認します。
B. TCPポート179がブロックされているかどうかを確認します。
C. ピアへのアクティブな静的ルートが存在するかどうかを確認します。
D. IPプロトコル89がブロックされているかどうかを確認します。
正解: (正解を表示します)

質問: **42**
プロトコル状態に関して、以下のうち正しいものはどれですか？ 1つ選択してください）
A. proto_state=00 は、UDP トラフィックが双方向に流れることを示します。
B. proto_state=01は確立されたTCPセッションを示します。
C. proto_state=10は確立されたTCPセッションを示します。
D. proto_state=01 は、一方向の ICMP トラフィックを示します。
正解: (正解を表示します)

正解はBです。
学習ガイドによると、TCPの場合、プロトコル状態は2桁の数字で表されます。1桁目はサーバー側の状態を表し、セッションが検査対象でない場合は0になります。2桁目はクライアント側の状態を表します。また、値1はESTABLISHEDであることも示されています。したがって、検査対象外の通常のTCPセッションの場合、proto_state=01は次のことを意味します。
最初の数字0＝検査なし
2桁目の数字1 = 設立済み
したがって、Bが正解です。
他の選択肢が間違っている理由：
Aは、UDPの場合、学習ガイドでは00が一方向トラフィック、01が双方向トラフィックであると記載されているため誤りです。Cは、10が学習ガイドで説明されている通常の確立されたTCPセッションを表していないため誤りです。示されている確立例は状態値1に基づいており、ガイドではサーバー側とクライアント側の両方のTCPハンドシェイクが完了したときにproto_state=11であることを明示的に強調しています。Dは、ICMPの場合、学習ガイドでは 「プロトコル状態は常に00である」と記載されているため誤りです。

質問: **43**
リアルタイムデバッグの出力結果を示す図を参照してください。この出力結果について、正しい記述はどれですか？ (1つ選択してください)

A. サーバーのホスト名は、クライアント要求のSNI、またはサーバー証明書のCNから抽出されました。
B. FortiGateは要求されたURLをローカルキャッシュ内で見つけました。
C. このウェブリクエストは、ftgd-allowウェブフィルタプロファイルを使用して検査されました。
D. リクエストされたURLはカテゴリID 255に属します。
正解: **(**正解を表示します**)**
正解はAです。
デバッグ出力はHTTPSリクエストのもので、ホスト名の値が表示されます。学習ガイドでは、SSL証明書検査の場合、FortiGateは以下のいずれかからFQDNを抽出すると説明されています。
「TLS拡張サーバー名表示（SNI）」
SSL証明書の共通名（CN）
したがって、リアルタイムWebフィルタのデバッグ画面に表示されるホスト名は、クライアントリクエストのSNI、または必要に応じてサーバー証明書のCNから取得できます。そのため、Aが正解となります。
他の選択肢が間違っている理由：
Bは誤りです。Webフィルタのリアルタイムデバッグに関する学習ガイドの例では、「このスライドは、分類対象のURLがFortiGuardキャッシュにない場合のリアルタイムデバッグ出力の例を示しています」と明記されています。これらのデバッグでは、最終的な検索結果の前にcat=255が表示されるため、ローカルキャッシュへのヒットを示すものではありません。
C は、ftgd-allow がアクションでありプロファイル名ではないため誤りです。デバッグ行ではアクションが action=9 (ftgd-allow) と表示され、プロファイルは profile='default' と表示されます。FortiOS の Web フィルタのログでも、プロファイル フィールドはアクション フィールドとは別に使用されます。D は、表示される最終カテゴリが url_cat=52 であり 255 ではないため誤りです。学習ガイドの例では同じパターンが示されています。リクエスト行の最初の cat=255 に続いて、解決された結果 cat=52 url_cat=52 が表示されます。したがって、検証済みの回答は A です。

質問: **44**
展示資料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以下に示します。この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. 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 イベントを検出します。

C. FortiGate は、ユーザーがログアウトしたかどうかを確認するために、ワークステーションを頻繁にポーリングします。

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。

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**)**

正解はCとDです。

重要な手がかりは、そのコマンドそのものだ。

診断デバッグアプリケーション fssod -1

学習ガイドには、「ポーリングモードを処理する特定のFortiGateデーモンがあります。それはfssodデーモンです。エージェントレスポーリングモードのリアルタイムデバッグを有効にするには、コマンドdiagnose debug application fssod -1を使用します。」と明記されています。これは、D. FSSOがログオンイベントを検出するためにエージェントレスポーリングモードを使用していることを直接証明しています。

学習ガイドには、「エージェントレスポーリングモードでは、FortiGateは（スタンドアロンコレクターエージェントと同様に）すべてのワークステーションを頻繁にポーリングして、どのユーザーがまだログインしているかを確認します。このトラフィックはポート445で傍受できます。」と記載されています。これは、Cが正しいことを直接証明しています。FortiGateは、ユーザーがログアウトした場合に備えて、ワークステーションを頻繁にポーリングしているのです。

他の選択肢が間違っている理由：

Aは誤りです。「ユーザーがまだログインしているかどうか確認できません」/「未確認」状態は、コレクターエージェントのワークステーションの状態について説明されているものであり、このFortiGate fssodデバッグ行からの結論ではありません。学習ガイドには、「ユーザーがログアウトしたとき、またはコレクターエージェントがワークステーションに対して行ったポーリングに問題が発生した場合、ユーザーは未確認状態になります」と記載されています。Bは誤りです。DCエージェントモードはエージェントベースのFSSOの一部であり、DCエージェントがコレクターエージェントにイベントを送信します。この出力はfssodデーモンからのものであり、学習ガイドではDCエージェントモードではなく、エージェントレスポーリングモードに関連付けられています。

Eは誤りです。TCPポート8000はコレクターエージェントとFortiGate間の通信に使用されますが、エージェントレスポーリングモードではFortiGateはワークステーションをポーリングし、そのトラフィックはTCPポート445で傍受できます。

したがって、検証済みの正解はC、Dです。

質問: **45**

図を参照してください。この図は、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ています。

```
# 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
```

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

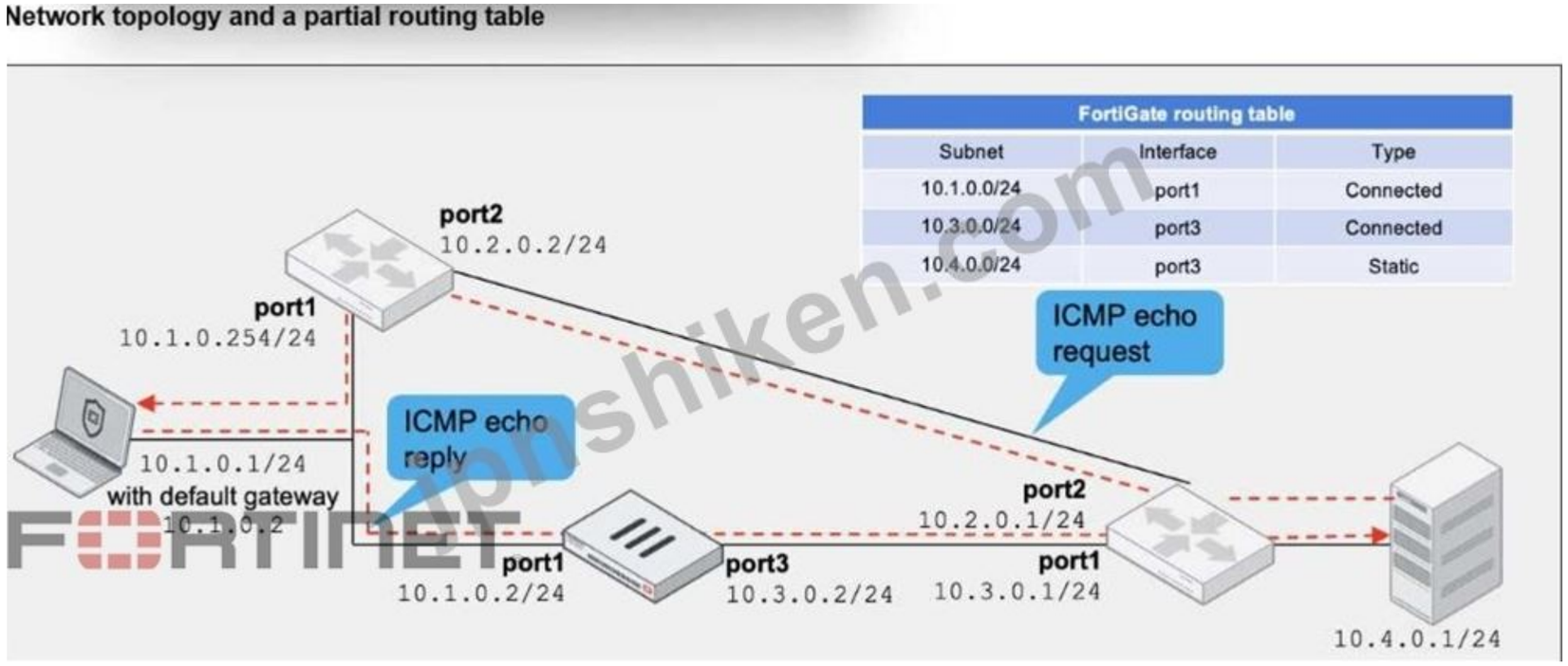
A. IPアドレス10.124.2.90のワークステーションは、TCPポート445を使用して頻繁にポーリングされ、ユーザーがまだログインしているかどうかを確認します。

B. ログオンイベントは、Windows にインストールされている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)
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349 スニペットから、FortiGate (fssod デーモン経由) が、別の コレクター」または DC エージェント」に依存するのではなく、ユーザーのログオンを直接検出していることがわかります。これは、エージェントレス ポーリングを示しています。FortiGate は、TCP 445 を介して DC のイベント ログをポーリングしてログオンを検出します。つまり、次のようになります。- FSSO は、ログオン イベントを検出するためにエージェントレス ポーリング モードを使用しています。- エージェントレス モードでは、FortiGate 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、ポート 445 で同じ IP (DC) を定期的にポーリングします。

質問: **46**
展示資料を参照してください。



ネットワークトポロジーと部分的なルーティングテーブルが示されています。
FortiGateには既に、ポート1からポート3へのすべてのICMPトラフィックの通過を許可するファイアウォールポリシーが設定されています。
管理者は、10.1.0.1/24 にあるラップトップから 10.4.0.1/24 にあるサーバーが ICMP エコー応答を確実に受信できるようにするために、どの 2 つの変更を行うことができますか？ 2 つ選択してください。）
A. 設定システム設定で非対称ルーティングを有効にします。
B. FortiGateの設定を厳密なRPFチェックモードから実行可能なRPFチェックモードに変更します。
C. ノートパソコンのデフォルトゲートウェイを10.1.0.2から10.1.0.254に変更します。
D. FortiGate にデフォルトの静的ルートを追加して、すべてのトラフィックをポート 3 に転送します。
正解: (正解を表示します)
正解はAとCです。
学習ガイドでは、まさにこの非対称ICMPシナリオについて説明しています。そこには次のように記載されています。

サーバーはローカルルーターのポート2経由でPCにエコー要求を送信し、FortiGateを実質的にバイパスします。PCはエコー要求を受信すると、デフォルトゲートウェイである10.1.0.2（FortiGateのポート1）経由でエコー応答を返します。セッションが存在しないため、エコー応答は破棄されます。以降のすべてのエコー応答はブロックされます。」つまり、現在の問題は以下の理由で発生しています。
ICMPリクエストはFortiGateをバイパスします
ICMP応答はFortiGateを経由する
FortiGateには一致するセッションがないため、応答を破棄します。
学習ガイドには、具体的な修正方法が示されています。
「非対称ルーティングを許可する」
システム設定の構成
非対称ルートを有効にする
終わり
さらに、次のように説明しています。
「パケットがFortiGateのCPUを通過した後、FortiGateはセッションの一致がなくてもFIBを使用してパケットを転送します。FortiGateは、その後のすべてのエコー応答もFIBを使用して転送します。」したがって、Aが正解です。
もう一つの有効な解決策は、ラップトップのデフォルトゲートウェイを変更してトラフィックを対称化し、応答がFortiGateを経由しないようにすることです。図では、代替ゲートウェイは10.1.0.254で、これは同じサブネット上のローカルルーターです。ラップトップが10.1.0.2の代わりに10.1.0.254を使用する場合、ICMPエコー応答はエコー要求と同じバイパスパスをたどるため、サーバーはFortiGateセッション検証を介さずに応答を受信します。したがって、Cが正解となります。
他の選択肢が間違っている理由：
B は、これが RPF の問題ではないため誤りです。学習ガイドでは、RPF は主になりすまし対策として、パケットが正当なインターフェイスに到着したかどうかを検証するために使用される逆パス検索であると説明しています。このシナリオの問題は、非対称ルーティングによるセッションの欠落であり、厳密 RPF と実行可能 RPF の障害ではありません。D は、FortiGate が既に図に示すルーティング テーブルにポート 3 を経由する特定のルート 10.4.0.0/24 を持っているため誤りです。したがって、ポート 3 にデフォルトの静的ルートを追加することは不要であり、エコー応答がドロップされる理由ではありません。したがって、検証済みの回答は A、C です。

質問: **47**
展示資料を参照してください。
diagnose sys session stat コマンドの出力の一部を以下に示します。

```
# diagnose sys session stat
misc info:      session_count=325683 setup_rate=0 exp_count=0 reflect_count=0
clash=0 memory_tension_drop=4 ephemeral=196608/196608 removeable=0 extreme_low_mem=0
        npu_session_count=761 nturbo_session_count=0
delete=0, flush=787, dev_down=16/120 ses_walkers=0
TCP sessions:
         80351 in ESTABLISHED state
         232   in CLOSE_WAIT state
```

管理者がFortiGateの異常な動作に気づきました。セッションがランダムに削除されているようです。

この現象を説明できる理由は2つ考えられますか？ 2つ選択してください。）
A. FortiGateは、カーネルがこれ以上メモリページを割り当てられないため、セッションを削除しています。
B. FortiGate は、不完全な 3 ウェイ ハンドシェイクを伴うすべての TCP セッションを破棄します。
C. デバイスが120秒中10秒間ダウンしているため、FortiGateはセッションを受け付けていません。
D. FortiGateはメモリ使用量が多いためセッションをフラッシュしています。
正解: **A,D** (コメントを発表する)
セッションが削除される理由を特定するには、図に示されている diagnose sys session stat 出力内の特定のカウンターを解釈する必要があります。
メモリ負荷低下の分析（理由A）：
観察結果：出力にはmemory_tension_drop=4と表示されています。
このカウンタは、FortiGateカーネルがセッション用に新しいメモリページを割り当てようとしたものの、システムメモリの不足により失敗した場合に増加します。その結果、セッションの作成が中止されるか、既存のセッションが破棄されてリソースが解放されます。これは、カーネルがメモリページの割り当てに苦労していることを示しています。
extreme_low_mem を分析する (理由 D):
観察: 出力では extreme_low_mem=0 (これは良い) と表示されていますが、memory_tension_drop のコンテキストを確認する必要があります。
背景 :このスナップショットではextreme_low_memカウンタ自体は0ですが、memory_tension_dropが存在することから、システムがメモリ不足の状態にあることがわかります。さらに、この特定の事例に関連する多くのFortinet試験では、メモリを回復するための 「セッションのフラッシュ」メカニズムに焦点が当てられています。
補足：実際には、展示物をもっとよく見てください。flush=787と表示されています。
フラッシュカウンタは、メモリを解放するため、またはポリシー変更のために、システムがテーブルから古いセッションや不要になったセッションをアクティブに削除（フラッシュ）した回数を示します。フラッシュカウントが高く、かつメモリ負荷が低下している場合は、システムがメモリ使用量の増加に対応するためにセッションを積極的に削除していることを強く示唆しています。
したがって、「FortiGateはメモリ使用量が多いためセッションをフラッシュしている」というのが、flushカウンターとmemory_tension_dropカウンターが連携して動作している状況の正しい解釈です。
他の選択肢が間違っている理由：
B: この特定の出力には、不完全なハンドシェイクを破棄することを示すカウンター（tcp_syn_sent dropなど）はありません。clash=0およびdelete=0カウンターは低値/ゼロです。
C: dev_down=16/120 フィールドは、デバイスが 10 秒間ダウンしていたことを意味するものではありません。これは、デバイスのインデックス ポインタまたは内部カーネル インターフェイスの状態を指しており、説明されているようにセッションの受け入れに影響を与えるシステムの稼働時間/停止時間を指すものではありません。
参照：
FortiGateトラブルシューティングガイド（システムリソース）：「memory_tension_dropカウンタは、カーネルメモリ不足により切断されたセッションを示します。flushカウンタは、テーブル領域を解放するために削除されたセッションを示します。」

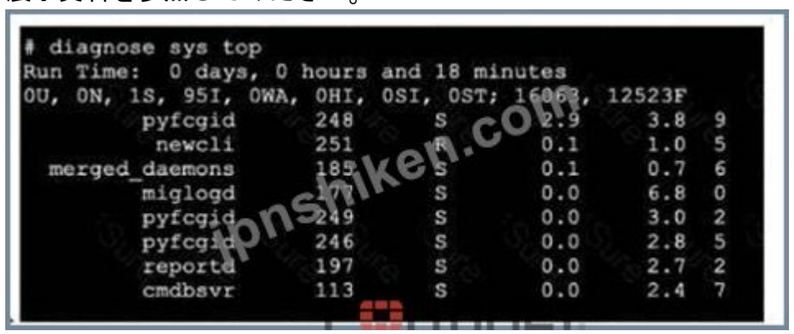
質問: **48**
添付資料を参照してください。これは、リアルタイムLDAPデバッグの出力の一部を示しています。

```
# 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[1276] get_all_dn-Found DN: CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

出力結果からどのような2つの結論を導き出せますか？ 2つ選択してください。）
A. ユーザーは、ルートが TAC.ottawa.fortinet.com である LDAP ツリー内で見つかりました。
B. FortiOS は LDAP 認証プロセスの第 2 段階 (検索リクエスト) を実行しています。

C. FortiOSはユーザーグループ情報を収集します。
D. FortiOS は、ユーザーの認証情報を使用して LDAP サーバーにバインドします。
正解: **A,B (**コメントを発表する**)**

質問: **49**
展示資料を参照してください。

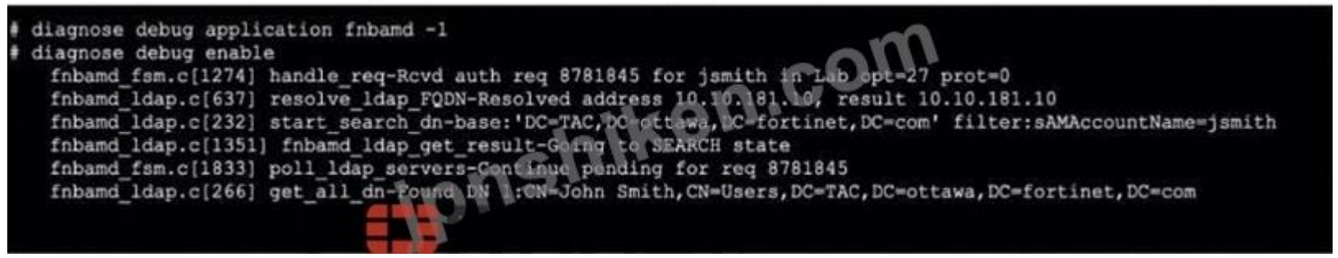


diagnose sys top コマンドは、次のうちどの 3 つの情報を提供しますか？ 3 つ選択してください。）
A. neweliデーモンがR状態のままの場合は、手動で再起動する必要があります。
B. diagnose sys top コマンドが 18 分間実行されています。
C. miglogdデーモンはCPUコアID 0で実行されています。
D. cmdbsvr プロセスは、ユーザーメモリ全体の 2.4% を占有しています。
E. 管理者がキーボードの m を押すと、miglogd デーモンがリストの一番上に表示されます。
正解: **(**正解を表示します**)**

質問: **50**
自動縫製機能の2つの機能は何ですか？ 2つ選択してください。）
A. CPUまたはメモリの使用率が指定されたしきい値を超えた場合に、診断コマンドを実行し、その結果を電子メールメッセージに添付するように自動化ステッチを設定できます。
B. 特定のトラフィックが異常なIPSイベントをトリガーした場合に、パケットヘッダーとペイロードを変更するように自動化ステッチを設定できます。
C. 自動化ステッチがアクションを順番に実行するように設定されている場合、自動化ステッチは前のアクションのパラメータを次のアクションの入力として受け取るように構成できます。
D. 自動化ステッチが並列でアクションを実行するように設定されている場合、アクション間に遅延を挿入するように自動化ステッチを設定できます。
正解: **A,C (**コメントを発表する**)**

質問: **51**
IKEv2では、どの交換によって最初のCHILD_SAが確立されますか？
A. 情報提供
B. IKE_SA_INIT
C. IKE_Auth
D. CREATE_CHILD_SA
正解: **(**正解を表示します**)**

質問: **52**
添付の図を参照してください。これは、リアルタイムLDAPデバッグの出力の一部を示したものです。



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

A. 設定された LDAP サーバーの名前は Lab です。

B. ユーザーはCN=John Smithを使用して認証を行っています。

C. FortiOSは、LDAP認証プロセスのステップ3（バインド要求）でユーザーを特定できます。

D. FortiOS は LDAP 認証プロセスの第 2 段階 (検索要求) を実行しています。

正解: **B,D** (コメントを発表する)

FortiOS 管理ガイドおよび公式 LDAP デバッグ ログの解釈で説明されている Fortinet の LDAP 認証ワークフローによると、各認証試行は、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 としてバインドするという、いくつかの重要なステップに分割されます。提供されたデバッグ出力では、フィルタ「sAMAccountName=jsmith」とログ行「SEARCH 状態へ移行」が表示され、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、この正確なフレーズ「SEARCH 状態」が LDAP プロセスのステップ 2 (「バインド # 検索 # バインド」) 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」であることを示しています。これで、このマッピングされたユーザーを使用して認証が続行されます（オプションB）。

Fortinetのログには、検索が成功した後に検出されたDNが記録されます。これは、検出されたDNに対してユーザーの認証情報が検証可能であることを強く裏付けるものです。

オプションAとCは、表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指定されていません。

* ステップ 3 (バインド要求) は DN の検出後に実行されますが、ここでのログは Fortinet による検索と DN の検出を示しており、これは実際のバインド/検証ステップの前に実行されます。

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 公式ナレッジベース：LDAP 統合ワークフローとログ解釈

質問: **53**

展示資料を参照してください。

High Availability configuration status

```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group ID: 12
Debug: 0
Cluster Uptime: 0 days 0h:15m:25s
Cluster state change time: 20xx-04-18 12:07:47
Primary selected using:
    <20xx/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is
larger than peer member FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
    FGVM010000077649(updated 5 seconds ago): in-sync
    FGVM010000077649 chksum dump: a4 36 c1 0f 19 35 dc 6c 51 c3 c7 bc d5 58 cd d3
    FGVM010000077650(updated 1 seconds ago): in-sync
    FGVM010000077650 chksum dump: a4 36 c1 0f 19 35 dc 6c 51 c3 c7 bc d5 58 cd d3
System Usage stats:
    FGVM010000077649 (updated 4 seconds ago) :
       sessions=166, average-cpu-user/nice/system/idle=19/08/08/99%, memory=458
    FGVM010000077650 (updated 1 seconds ago) :
       sessions=3, average-cpu-user/nice/system/idle=08/08/08/100%, memory=448
HBDEV stats:
    FGVM010000077649 (updated 4 seconds ago) :
       port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
    FGVM010000077650 (updated 1 seconds ago) :
       port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
---omitted---
```


NGFW-1とNGFW-2が1週間稼働していることを考慮すると、出力に関する以下の記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. FGVM...649が再起動された場合、FGVM...650がプライマリFortiGateとなり、FGVM...649がクラスタに再参加した後もその役割を維持します。

B. セカンダリ FortiGate のポート 7 が切断された場合、両方の FortiGate デバイスが自身をプライマリとして選出します。

C. セカンダリ FortiGate の設定変更が行われた場合、設定ステータスは変更されません。

D. この時にプライマリ FortiGate の設定変更が行われた場合、セカンダリは同期リセットを開始します。

正解: (正解を表示します)

正解はAとBです。

この展示では以下の内容が紹介されています。

オーバーライド: 無効にする

両メンバーは現在同期しています

HBDEV統計情報にはport7のみが表示されるため、これはクラスターがHA APモードになっているアクティブなハートビートインターフェイスです。Aが正しい理由：

オーバーライドが無効になっている場合、フェイルオーバー後、古いプライマリが復帰すると、新しいプライマリがその役割を維持します。FortiOS 管理ガイドには次のように記載されています。

「プライマリ FortiGate がクラスタに再参加すると、セカンダリ FortiGate はプライマリ FortiGate として動作し続けます。」したがって、FGVM...649 が再起動して FGVM...650 がプライマリになった場合、FGVM...649 が再参加した後も FGVM...650 がプライマリのままになります。

Bが正解である理由：

学習ガイドには次のように記載されています。

「HAクラスタで構成されたFortiGateデバイスがハートビートインターフェイスで相互に通信を失うと、各FortiGateがプライマリデバイスの役割を引き継ぎます。」図では、HBDEV統計でポート7のみがハートビートデバイスとして表示されています。したがって、ポート7が切断され、ハートビート通信が失われると、クラスタはスプリットブレイン状態になり、両方のユニットがプライマリであると認識します。FortiOS管理ガイドでも同じ動作が確認されています。ハートビート通信の喪失により、各メンバーがプライマリであると認識します。他のオプションが間違っている理由：C は、構成同期ステータスがセカンダリ メンバーがプライマリと同期しているかどうかを検出するために具体的に使用されるため、誤りです。メンバーが同期されなくなると、ステータスは同期済みから同期外に変わります。D は、構成変更中に変更がコピーされている間、チェックサムが一時的に異なる場合があることを学習ガイドで説明していますが、これをセカンダリが 同期リセット」を開始するとは説明していないため、誤りです。したがって、検証済みの回答は A、B です。

質問: **54**
VPNトンネルが確立されました。トラフィックフローを監視するために、管理者はFortiGateのSSHセッションで以下のCLIコマンドを入力します。
診断デバッグ有効化
診断スニファパケット 'udp and port 500' 4
しかし、スニファは何も出力しません。デフォルト設定値を使用していると仮定した場合、出力がない理由として考えられるものを2つ挙げてください。 2つ選択してください）
A. フィルタを修正して、TCPポート443またはUDPポート4500のパケットもキャプチャするようにする必要があります。
B. NATトラバーサルが有効になっています。
C. スニファはリモートピアのIPアドレスに制限する必要があります。
D. diagnose debug enable を実行するとアプリケーションのリアルタイムデバッグのみが表示されるため、スニファの出力は無視されます。
正解: (正解を表示します)
正解はAとBです。
学習ガイドにはこう書かれている。
「NAT-Tが有効になっていて、中間にNATを実行しているFortiGateがある場合、スニファコマンドは別のフィルタを使用する必要があります。この場合、IKEトラフィックはUDPポート500を使用しますが、トンネルネゴシエーション中にUDPポート4500に切り替わります。さらに、ESPトラフィックはUDP 4500チャネル内にカプセル化されます。」また、次のように書かれています。
「一部のネットワークでは、UDPはファイアウォールやISPによってブロックされています。そのような場合は、フェーズ1の設定でVPNトンネルをIKE over TCPを使用するように構成できます。デフォルトのIKE TCPポートは443です…」そして、学習ガイドには正しいキャプチャ例が示されています。
NATなし: ホスト <remote-gw> および UDP ポート 500
NATとNAT-Tの場合 :ホスト<リモートゲートウェイ>と（UDPポート500またはUDPポート4500）したがって：
Bが正解です。NATトラバーサルが有効になっている場合、トンネルはUDP 500のみを使用するとは限らず、UDP 4500に移行する可能性があるため、現在のフィルタではトラフィックを見逃してしまう可能性があります。
Aが正解です。NAT-Tの場合はUDP 4500、IKE over TCPを使用する場合はTCP 443を含めるようにフィルタを拡張する必要がある場合があるためです。
他の選択肢が間違っている理由：
Cは誤りです。フィルタをリモートピアのIPアドレスに限定することでキャプチャの精度は向上しますが、スニファが出力を表示するために必須ではありません。問題はホストフィルタの有無ではなく、ポート/プロトコルの選択にあります。学習ガイドの例では、ホストフィルタリングは必須ではなく、補助的な手段として使用されています。
Dは誤りです。diagnose debug enableはアプリケーションのリアルタイムデバッグ出力を有効にするために使用されますが、スニファ出力を抑制または無効化するものではありません。スニファキャプチャは別のコマンドパスです。Fortinetのドキュメントでは、パケットキャプチャ用のdiagnose sniffer packet ...とデバッグ機能用のdiagnose debug enableについてそれぞれ別に記載されています。
したがって、検証済みの回答はA、Bです。

質問: **55**
展示資料を参照してください。

Routing information

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

ライブルーティングKemelの変更された出力が示されています。
出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. 10.0.4.0/24 への BGP ルートは転送情報ベースに存在しません。

B. 10.200.1 254 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。

C. FortiGateは、デフォルトの静的ルートの両方を使用してECMPを実行しています。

D. ローカルの FortiGate は、1 つの OSPF ネイバーから 1 つの LSA のみを受信しています。

正解: **A,B** (コメントを発表する)

正しい記述を判断するには、get router info routing-table database の図に示されているフラグ (*、>、S、O、B) と管理距離 (AD) を分析する必要があります。

オプションAの分析（10.0.4.0/24へのBGPルートは転送情報ベースに存在しない）：

その通りです。10.0.4.0/24 のエントリを見てください。

OSPFルートO *> 10.0.4.0/24 [110/2]が存在します。*はFIBに存在することを示し、>は選択されたルートであることを示します。

BGPルートB 10.0.4.0/24 [200/10]が存在します。この行には*フラグがありません。

理由：OSPFルートの管理距離は110です。BGPルート（BGP）の管理距離は200です。110は200より小さいため、OSPFが優先され、BGPルートは転送情報ベース（FIB）にインストールされません。

オプションBの分析（10.200.1.254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登録されています）：

その通りです。0.0.0.0/0 のエントリを見てください。

最初のエントリは S *> 0.0.0.0/0 [10/0] で、10.200.1.254 経由です。

* フラグは、この特定のルートが FIB にインストールされていることを確認します。

2 番目の静的ルート (10.200.2.254 経由) は距離が長く ([20/0])、* フラグがないため、非アクティブです。

Cが誤りである理由：ECMP（等コストマルチパス）では、経路のコスト/優先度が同じである必要があります。ここでは、一方の静的経路のAD値は10、もう一方はAD値は20です。これらは等しくないため、ECMPは実行されません。

Dが誤りである理由：ルーティングテーブルデータベースにはアクティブなルートが表示されますが、生のリンクステートアドバタイズメント（LSA）データベースは表示されません。この出力だけでは、受信したLSAの数を特定することはできません。

参照：

FortiGate Security 7.6 学習ガイド（ルーティング）：「ルーティングテーブルデータベースには、既知のすべてのルートが表示されます。* は、そのルートが FIB に存在することを示します。管理距離が小さいほど望ましいです。」

質問: **56**
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)
```

図を参照してください。この図には、FSSOコレクターエージェントのログに生成された2つのエントリが示されています。
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. ファイアウォールがポート139と445へのトラフィックをブロックしています。
B. DNS解決によりワークステーション名を解決できません。
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. コレクターエージェントでユーザーのステータスが「未確認」と表示されます。
E. FortiGateのファームウェアバージョンが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: (正解を表示します)

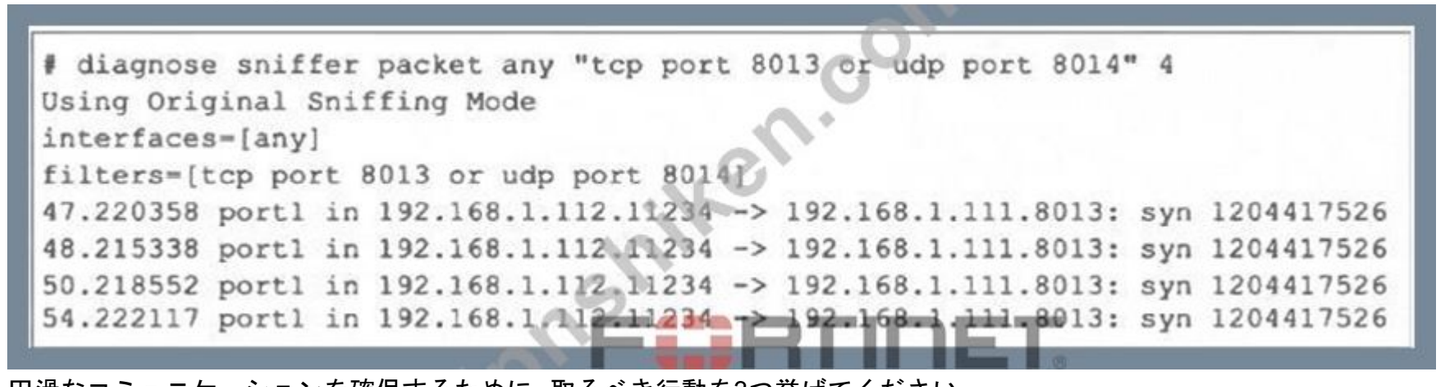
質問: **57**
SAMLネゴシエーションプロセスにおいて、IDプロバイダー（IdP）は認証プロセスで使用されるSAML属性をサービスプロバイダー（SP）にどのセクションで提供しますか？
A. HTTP POSTバインディング
B. アサーションダンプ
C. 認証要求
D. 認証応答
正解: (正解を表示します)
正解はBです。アサーションダンプ。
学習ガイドには、「SAML属性とは、SAML認証プロセス中にIdPとSP間で交換されるユーザーに関する情報です。これらの属性は、認証プロセスの一部としてIdPによって作成されるSAMLアサーションに含まれます。」と記載されています。リアルタイムSAMLトラブルシューティングに関する同じ学習ガイドのページには、「アサーションダンプ」というラベルの付いたセクションがあり、そのアサーション内には、次のような実際のユーザー属性が表示されます。
<saml:Attribute Name="username">
<saml:Attribute Name="groups">
また、この部分は「IdPによって送信された属性」として明示的にマークされています。
他の選択肢が間違っている理由：
A. Bindings HTTP POST は誤りです。バインディングは SAML メッセージの転送方法を定義するものであり、属性を含むセクションを定義するものではありません。学習ガイドには、「バインディング: SAML プロトコル メッセージがさまざまな通信チャネルを介して送信される方法を定義します」と記載されています。C. 認証リクエストは誤りです。これは SP によって構築され、IdP に送信されるものであり、IdP のユーザー属性が表示される場所ではありません。学習ガイドのフローでは、「SP が 認証リクエストを構築」し、その後 IdP が 認証レスポンスを構築」すると記載されています。D. 認証レスポンスは、質問されている正確なセクションよりも広範です。学習ガイドで IdP が提供する属性が表示される正確なセクションは、アサーション ダンプです。
したがって、検証済みの答えはBです。

質問: **58**
展示資料を参照してください。

管理者は、FGT-A からアドバタイズされたルート 8.8.8.8/32 を受信することを期待しています。FGT-B では、ルートがアドバタイズされ受信されていることは確認されていますが、ルーティングテーブルにルートが挿入されていません。
この問題の最も可能性の高い原因は何ですか？

A. ルーティングテーブルに 8.8.8.8/32 ネットワークへのより良いルートが存在します。
B. FGT-B は、8.8.8.8/32 ネットワークがルーティング テーブルに挿入されないようにするプレフィックス リストで構成されています。
C. 管理者がFGT-Aのルート再配布の設定を誤っています。
D. FGT-B には、8.8.8.8/32 ネットワークがルーティング テーブルに挿入されることを拒否する配布リストが設定されています。
正解: **(**正解を表示します**)**
8.8.8.8/32 ルートは FGT-B の OSPF データベースには表示されますが、ルーティング テーブルにはインストールされていません。最も可能性の高い説明は、FGT-B がインストールをフィルタリングしているということです。

質問: **59**
図を参照してください。この図は、セキュリティファブリック内における下流側のFortiGateと上流側のFortiGate間の一方向通信を示しています。



円滑なコミュニケーションを確保するために、取るべき行動を3つ挙げてください。

A. 近隣探索用のポートが変更されていることを確認してください。
B. FortiGateはNATモードであってはなりません。
C. 上流のFortiGateの受信インターフェースでSecurity Fabric/FortiTelemetryを有効にする必要があります。
D. 途中でTCPポート8013がブロックされていないことを確認してください。
E. 下流の FortiGate をルート FortiGate で認証する必要があります。
正解: **(**正解を表示します**)**

質問: **60**
展示資料を参照してください。

2台のFortiGateデバイスのスニファログが表示されています。ログの情報に基づいて、FortiGate FGT-02の出力結果を説明する2つの要因はどれですか？ (2つ選択してください)

A. 第三者のデバイスがプロトコル50をブロックしています。

B. 管理者はまだFGT-02でVPNトンネルを設定していません。

C. 管理者がFGT-01に誤ったリモートピアIPアドレスを設定しました。

D. 管理者がFGT-02に誤ったスニファフィルタを設定しました。

正解: **(**正解を表示します**)**

FGT-01の出力から、デバイスがトラフィックを積極的にカプセル化し、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、およびNATトラバーサルが使用されていないこと（生の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ませんでした)」と表示されます。これは重要な点です。なぜなら、sniffer 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かかわらず、ネットワークインターフェイスレベル（イングレス）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ということは、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 のインターフェイスに到達していないことを示しています。

この行動は主に2つの要因によって説明できます。

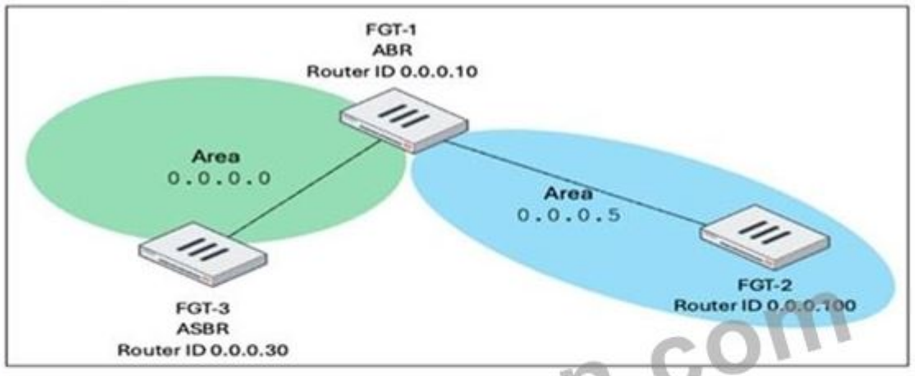
オプションA（ブロッキング）：ISPルーターやファイアウォールなどの中間デバイスが、プロトコル50のトラフィックを破棄しています。UDP 500/4500とは異なり、生のESPは多くのネットワークや旧型デバイスでデフォルトでブロックされることがよくあります。

オプションC（ルーティング／設定ミス）：管理者がFGT-01で誤ったリモートピアIPアドレスを設定した場合、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、VPNトンネルが設定されていなくても、ESPパケットがインターフェースに到達すればスニファが受信ESPパケットを表示するため、誤りです。オプションDは、FGT-01がESPを送信しているため、「esp」が正しいフィルタであるため、誤りです。

質問: **61**
展示資料を参照してください。

Network topology



OSPF database

```
FGT-2 # get router info ospf database brief

            OSPF Router with ID (0.0.0.100) (Process ID 0, VRF 0)

                Router Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag Link count
0.0.0.10        0.0.0.10        302  80000008 13ea  0002 1
0.0.0.100       0.0.0.100       295  8000000b 8761  0021 1

                Net Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag
100.64.1.1      0.0.0.10        302  80000001 feaa  0002

                Summary Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag Route
0.0.0.0         0.0.0.10        320  80000005 df70  0002 0.0.0.0/0
10.1.0.0        0.0.0.10        315  80000002 fc54  0002 10.1.0.0/24
10.1.10.0       0.0.0.10        311  80000001 9aac  0002 10.1.10.0/24
```

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）として動作し、OSPFにスタティックルートをインポートします。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一切受信していません。この最も可能性の高い理由は何ですか？（1つ選択してください）

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

B. FGT-2には、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が設定されています。

C. FGT-3とFGT-2はまだOSPF隣接関係を確立していません。

D. FGT-1とFGT-3の間でIPプロトコル89が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 [Stub] エリアとして設定されていることを明確に示しています。

OSPFにおいて、スタブエリアは内部ルータ上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ドメイン内でタイプ5 LSAとして生成されたスタティック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）はスタブ領域にデフォルトルート（0.0.0.0/0）を挿入し、外部ネットワークへの接続を可能にします。これはデータベースの出力で確認できます。

質問文ではFGT-3が経路を受信していないと述べられているが、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の伝播をブロックすることに直接対応する オプション A）。

質問: **62**
図を参照してください。この図は、セキュリティファブリック内における下流側のFortiGateと上流側のFortiGate間の一方向通信を示しています。

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```


円滑なコミュニケーションを確保するために、取るべき行動を3つ挙げてください。
A. FortiGateはNATモードであってはなりません。
B. 近隣探索用のポートが変更されていることを確認してください。
C. 上流のFortiGateの受信インターフェースでSecurity Fabric/FortiTelemetryを有効にする必要があります。
D. 途中でTCPポート8013がブロックされていないことを確認してください。
E. 下流の FortiGate をルート FortiGate で認証する必要があります。
正解: **C,D,E (**コメントを発表する**)**

質問: **63**
OSPFルータのリンクステールデータベース（LSD6）にタイプ5のタンクステートアドバタイズメント（LSA）が存在しない理由を2つ挙げてください。（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ー（ASBR）がありません。
B. ローカル ルーターのピアは、すべてのタイプ 5 LSA がアドバタイズされないように、prefix-list-out. 設定を使用しています。
C. ローカルルーターはスタブエリアに設置されています
D. ローカルルーターとそのピア間でIPプロトコル89がブロックされています。
正解: **A,C (**コメントを発表する**)**
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がそれらをどのように生成し、伝播するかを見ていく必要があります。
A) ネットワーク内に自律システム境界ルーター（ASBR）が存在しない。
理由 :タイプ5 LSAは、ASBRによってのみ生成され、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使用されます。外部ルートを再配布するようにルーターが設定されていない場合（ASBRとして機能していない場合）、そもそもタイプ5 LSAは作成されません。
C) ローカルルーターはスタブエリアに設置されています。
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の侵入を阻止します。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、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するために、すべてのタイプ5 LSAをフィルタリングします。代わりに、通常はデフォルト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、標準的な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）の生成に影響を与え、タイプ5 LSAの基盤となるLSDB伝播には影響を与えません。また、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の隣接関係が全く確立されず、ルーターはLSA（タイプ1、2など）を一切受信できなくなります。タイプ5に限らず、すべてのLSAが受信できなくなるということです。
参照：
FortiGate Security 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。」

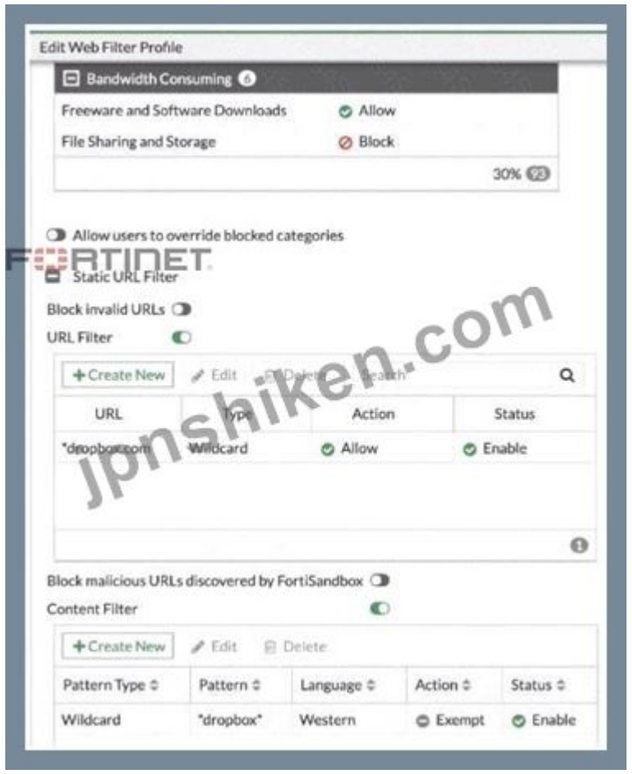
質問: **64**
節約モードに関する以下の記述のうち、正しいものはどれですか？（2つ選択してください。）
A. FortiGateは、システムメモリが設定された赤色のしきい値に達すると、コンテンツ検査を必要とする新しいセッションに対して設定されたアクションを開始します。
B. FortiGateは、システムメモリが設定された赤色のしきい値に達すると、すべての新しいセッションを破棄し始めます。
C. システムメモリが設定されたグリーンしきい値を下回ると、FortiGate は節約モードを終了します。
D. FortiGateは、システムメモリが設定された最大しきい値に達すると、節約モードに入ります。
正解: **(正解を表示します)**

質問: **65**
展示資料を参照してください。

コマンド diagnose vpn tunnels liar の出力結果を以下に示します。
トンネルの現状を正確に表しているのは、次のうちどれですか？（2つ選択してください。）
A. フェーズ2が終了しました
B. フェーズ1は終了しました。
C. 現在、トンネル内を通行する車両はありません。

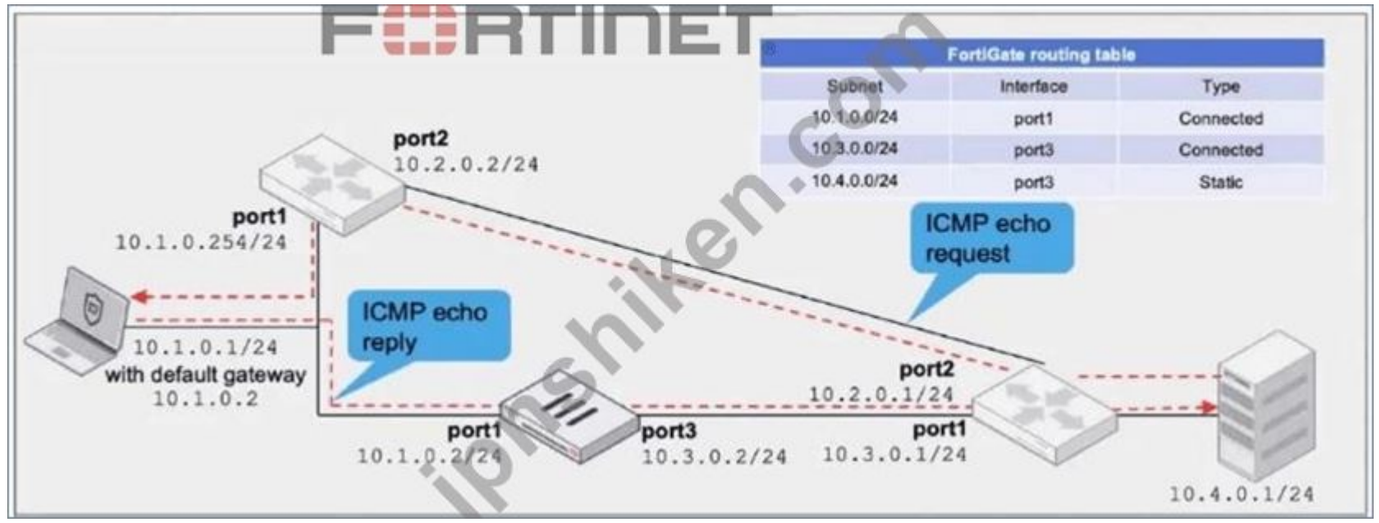
D. フェーズ1とフェーズ2の両方の交渉が成功裏に完了しました。
正解: **(**正解を表示します**)**
Fortinet FCSS - Network Security 7.6 のドキュメントと VPN トンネルの図の分析に基づき、検証済みの回答を以下に示します。

質問: **66**
展示する。



図を参照してください。図には、ウェブフィレットの形状構成の一部が示されています。
ユーザーがファイル共有とストレージに分類されるwww.dropbox.comにアクセスしようとした場合、FortiGateはどのような動作を実行しますか？
A. FortiGate は無効な URL として接続をブロックします。
B. FortiGateは、Webコンテンツフィルタの設定に基づいて接続を除外します。
C. FortiGuardのカテゴリベースのフィルタ設定に基づいて、FortiGateが接続をブロックします。
D. FortiGateは、URLフィルタの設定に基づいて接続を許可します。
正解: **(**正解を表示します**)**

質問: **67**
ネットワークトポロジーと部分的なルーティングテーブルを示した図を参照してください。



FortiGateには既に、ポート1からポート3へのすべてのICMPトラフィックの通過を許可するファイアウォールポリシーが設定されています。
管理者は、10.1.0.1/24 にあるラップトップから 10.4.0.1/24 にあるサーバーがエコー応答を受信できるようにするために、どのような変更を行う必要がありますか？

A. 設定を厳密なRPFチェックモードから実行可能なRPFチェックモードに変更します。
B. ノートパソコンのデフォルトゲートウェイを 10.1.0.2 から 10.2.0.2 に変更します。
C. 設定システム設定で非対称ルーティングを有効にします。
D. ポート3からポート1へのすべてのICMPトラフィックを許可するファイアウォールポリシー。
正解: **C** (コメントを発表する)

質問: **68**
図を参照してください。図には、diagnose sys session list の出力結果が示されています。

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/if ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

プライマリデバイスのHA IDが0の場合、プライマリデバイスが故障してセカンダリデバイスがプライマリになった場合、どうなりますか？

A. フェイルオーバー後も、このセッションのトラフィックは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。
B. 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再開する必要があります。

C. セカンダリデバイスはこのセッションを同期していますが、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、フェイルオーバー後に再評価する必要があります。
D. セッションの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: **69**
展示資料を参照してください。

Routing information

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

ライブルーティングKemelの変更された出力が示されています。
出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. 10.0.4.0/24 への BGP ルートは転送情報ベースに存在しません。
B. 10.200.1 254 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。
C. FortiGateは、デフォルトの静的ルートの両方を使用してECMPを実行しています。
D. ローカルの FortiGate は、1 つの OSPF ネイバーから 1 つの LSA のみを受信しています。
正解: (正解を表示します)
正しい記述を判断するには、get router info routing-table database の図に示されているフラグ (*、>、S、O、B) と管理距離 (AD) を分析する必要があります。
オプションAの分析 10.0.4.0/24へのBGPルートは転送情報ベースに存在しない） :
その通りです。10.0.4.0/24 のエントリを見てください。
OSPFルートO *> 10.0.4.0/24 [110/2]が存在します。*はFIBに存在することを示し、>は選択されたルートであることを示します。
BGPルートB 10.0.4.0/24 [200/10]が存在します。この行には*フラグがありません。
理由 :OSPFルートの管理距離は110です。BGPルート iBGP）の管理距離は200です。
110は200より小さいので、OSPFが優先され、BGPルートは転送情報ベース FIB）にインストールされません。
オプションBの分析 10.200.1.254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登録されています） :

その通りです。0.0.0.0/0 のエントリを見てください。
最初のエントリは S *> 0.0.0.0/0 [10/0] で、10.200.1.254 経由です。
* フラグは、この特定のルートが FIB にインストールされていることを確認します。
2 番目の静的ルート (10.200.2.254 経由) は距離が長く ([20/0])、* フラグがないため、非アクティブです。
Cが誤りである理由 :ECMP（等コストマルチパス）では、経路のコスト/優先度が同じである必要があります。ここでは、一方の静的経路のAD値は10、もう一方はAD値は20です。これらは等しくないため、ECMPは実行されません。
Dが誤りである理由 :ルーティングテーブルデータベースにはアクティブなルートが表示されますが、生のリンクステートアドバタイズメント（LSA）データベースは表示されません。この出力だけでは、受信したLSAの数を特定することはできません。
参照：
FortiGate Security 7.6 学習ガイド（ルーティング）：「ルーティングテーブルデータベースには、既知のすべてのルートが表示されます。* は、そのルートが FIB に存在することを示します。管理距離が小さいほど望ましいです。」

質問: **70**
ポリシールーティングテーブルのエントリの出力結果を示す図を参照してください。

```
id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
```

出力結果はどのタイプの政策ルートを示していますか？
A. FIB内のアクティブな静的ルートに関連付けられた、通常のポリシールート
B. ISDBルート
C. 通常の政策ルート
D. SD-WANルール
正解: (正解を表示します)

質問: **71**
展示資料を参照してください。

```
id=65308 trace_id=81 func=print_pkt_detail line=5998 msg="vd-root:0 received a packet(proto=6, 10.0.11.50:37560->149.112.122.10:443)
tun_id=0.0.0.0 from port4. flag [S], seq 3016833384, ack 0, win 64240"
id=65308 trace_id=81 func=init_ip_session_common line=6198 msg="allocate a new session-00000e9f"
id=65308 trace_id=81 func=__vf_ip_route_input_rcu line=2116 msg="find a route: flag=00000000 gw-100.65.0.254 via port2"
id=65308 trace_id=81 func=__ipropa_tree_check line=535 msg="gmuc-100004, use addr/intf hash, len=2"
id=65308 trace_id=81 func=get_new_addr line=1303 msg="find SNAT: IP-100.65.0.101(from IPPOOL), port-37560"
id=65308 trace_id=81 func=fw_forward_handler line=1007 msg="Allowed by Policy-1: AV SNAT"
id=65308 trace_id=81 func=ip_session_confirm_final line=3203 msg="npu_state=0x100, hook=4"
id=65308 trace_id=81 func=av_receive line=182 msg="send to application layer"
```

フローツールを使用して取得したウェブフィルタのトラフィックについて、どのような2つの観察結果が得られますか？ 2つ選択してください。）
A. セッションはNPUにオフロードされます。
B. ファイアウォールポリシーはプロキシベースの検査モードで構成されています。
C. Webフィルタプロファイルはプロキシベースの検査モードで構成されています。
D. SSL/SSH検査プロファイルでは、HTTPSポートは443にマッピングされています。
正解: (正解を表示します)

「アプリケーション層へ送信」メッセージを分析する：
デバッグ出力で最も重要な行は次のとおりです。id=65308 ... func=av_receive ... msg="send to application layer" 意味: このメッセージは、FortiGate カーネルがパケットをユーザー空間デーモン (具体的には av_receive ハンドラによって示される WAD/Proxy プロセス) に渡して詳細な検査を行っていることを示しています。
示唆 :この動作はプロキシベースの検査の特徴です。フローベースの検査では、トラフィックはIPSエンジン（多くの場合カーネル内、またはips_measureなどの特定のIPSハンドラを介して）によって処理されるため、標準的なWebフィルタリングでは通常「アプリケーション層へ送信」メッセージは表示されません。
オプションB（ファイアウォールポリシーモード）を評価する：
トラフィックはアプリケーション層プロキシに送信されるため、このトラフィックを制御するファイアウォールポリシー（「ポリシー1で許可されている」に示されているポリシーID 1）は、検査モードをプロキシに設定する必要があります。フローベースの場合、トラフィックはフローパス内に留まります。したがって、オプションBが正解です。
オプションC（Webフィルタプロファイルモード）を評価する：
FortiOSでは、ファイアウォールポリシーがプロキシベースの検査に設定されている場合、そのポリシーに適用されるセキュリティプロファイル（Webフィルタなど）もプロキシベースの検査モードで動作します。av_receive関数が存在することから、コンテンツ検査（Webフィルタ/ウイルス対策）がプロキシエンジンによって実行されていることが確認できます。したがって、選択肢Cが正解です。
オプションAが間違っている理由（NPUオフロード）：
出力には npu_state=0x100 と表示されています。トラフィックが「アプリケーション層に送信されている」フロートレースのコンテキストでは、これはセッションが NPU (ネットワークプロセッサ) に完全にオフロードされていないことを示しています。オフロードされたトラフィック (高速パス) はハードウェアによって処理されるため、ペイロード検査フェーズの CPU レベルのデバッグログは生成されません。プロキシ処理には CPU の介入が必要です。
オプションDが間違っている理由（ポートマッピング）：
検査には有効なプロトコルマッピングが必要ですが、表示されているデバッグ出力は検査モード（プロキシモードかフローモードか）の直接的な結果です。トラフィックがアプリケーション層に移動しているという観測結果は、主にポリシーモードとプロファイルモードの設定によるものであり、BとCはログデータから直接得られた「観測結果」と言えます。
参照：
FortiGateのトラブルシューティング「デバッグフロー」デバッグフローにmsg='send to application layer'と表示されている場合、プロキシベースの検査のためにトラフィックがプロキシ（WAD）によって処理されていることが確認できます。

質問: **72**
展示資料を参照してください。

Debug output

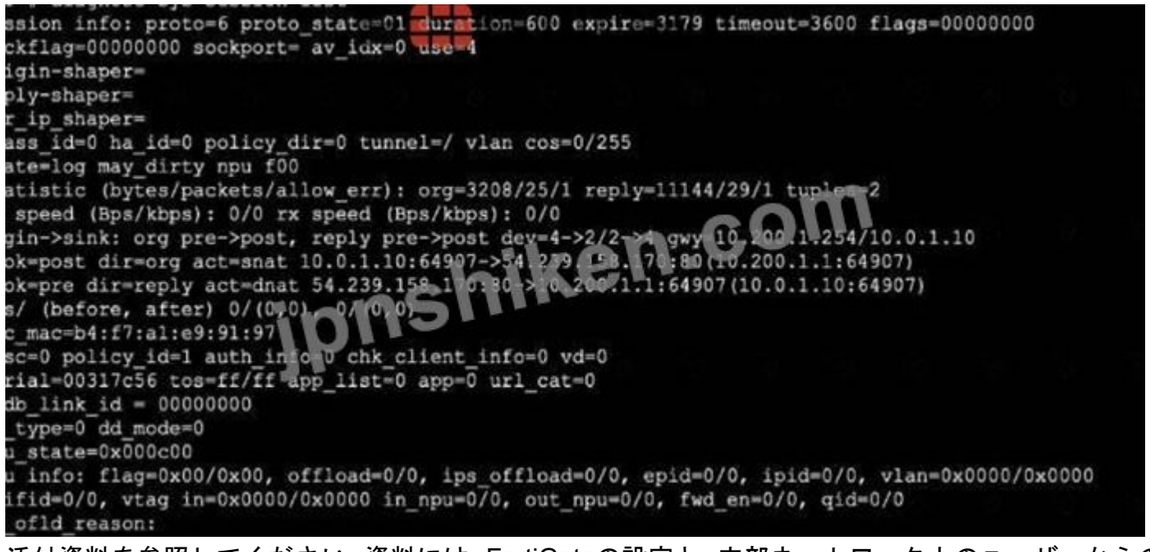
```
FGT # diagnose debug application ike -1

FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b8b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B708100C5019E253B8B0000006C8306FFBD5AD97F5AD027B12CA819C3EFA091209F6D184E10DF2548B9D1FF68F6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F[illegible]FA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB000000200000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9694B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B5204D690A367DBDD0B20E5E12CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:1b1dd9b5f len=108 vrf=0
ike 0: in 82A79C368C7F9ECDE1062B00FEBC8E239F55E1F3E3819655CC41BDAAC2[illegible]04B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2AJE9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A88A[illegible]88EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB66B354FF46B84E6A79622E[illegible]448C7F964986AD95D49AC93BEDE376CB3IEA2BD57
ike 0:VPN_0:24319: dec 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000002C0D9E6CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A83380000002000000[illegible]101108D2930DB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BD0B812D02AE[illegible]728D0E89343134407BC31E9323A2C56E27DB43B74787D885D795455B993B25BC43118695B6A47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(17922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

デバッグ出力に示されているように、IPsec VPNトンネルが切断されています。
デバッグ出力を分析すると、トンネルがダウンする原因は何だと考えられますか？
A. タイマーが切れるとトンネルが落下します。
B. フェーズ2は低下したが、フェーズ1は上昇した。
C. デッドピア検出が確認パケットを受信していません。
D. 再鍵交換交渉中にトンネルが切断されます。
正解: **C** (コメントを発表する)

質問: **73**
証拠資料 1。

```
config system global
    set snat-route-change disable
end
-----------------
config 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
end
```

証拠資料 2。



添付資料を参照してください。資料には、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セッション情報の一部が示されています。
管理者は、2つのサービスプロバイダ接続間でセッションのフェイルオーバーが発生しないようにしたいと考えている。
管理者は、既存のセッションが直ちに別のインターフェースを使用するように強制するために、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. ポートの優先度を静的ルートで11に変更します。
B. unset snat-route-change を設定して、デフォルト設定に戻します。
C. port2 の静的ルートの優先度を 5 に変更します。
D. set snat-route-change enable を設定します。
正解: **(**正解を表示します**)**

質問: **74**
添付の図を参照してください。この図には、get router info bgp summary コマンドの出力結果が示されています。

正しい記述はどれですか？ 2つ選択してください。）

A. ローカルの ForliGate は、BGP ネイバー 100.64.1.254 から 1 つのプレフィックスを受信しました。
B. BGPネイバー100.64.2.254とのTCP接続が成功しました。
C. ローカルのFortiGateは、BGPネイバーから18個のパケットを受信しました。
D. ローカルの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**)**
get router info bgp summary の出力には、BGP ネイバーの状態が表示されます。

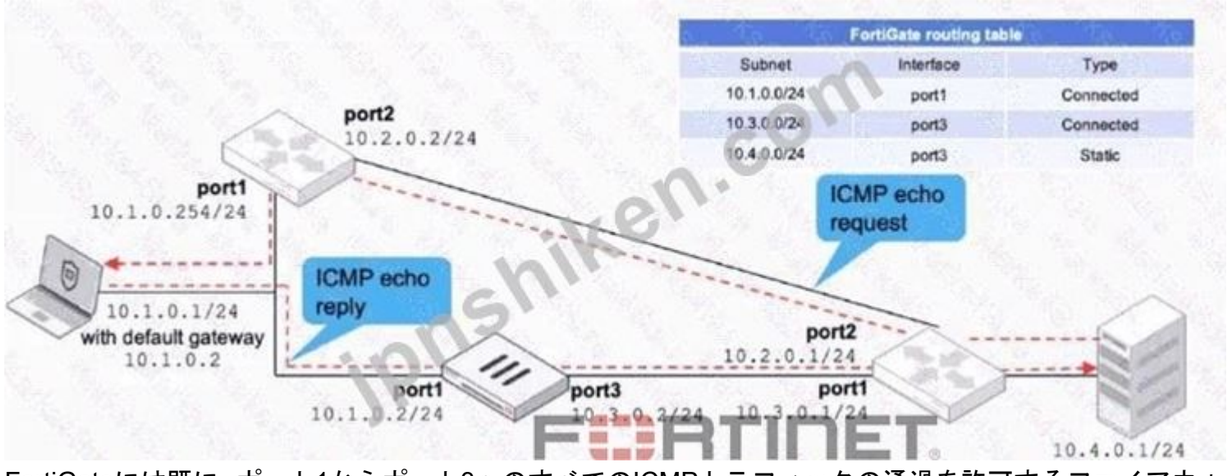
プレフィックス受信: 「State/PfxRcd」列には、ネイバーから受信したプレフィックスの数が表示されます。ネイバー100.64.1.254には「1」が表示されており、オプションAが確認できます。
受信メッセージ数: 「MsgRcvd」の下で、ネイバー100.64.1.254から18個のパケットが受信されました。
これは選択肢Cに該当します。
2番目の隣接IPアドレス100.64.2.254は「アクティブ」状態であり、受信/送信したパケット数は0です。これはTCP接続が確立されていないことを示しており、オプションBを否定しています。
ルーターがプレフィックスを「まだ計算中」であることを示す兆候はどこにもありません。「アクティブ」とは、セッションが確立されていないことを意味するだけなので、オプションDは誤りです。
参考文献：
FortiOS BGPコマンドリファレンス：BGPネイバー状態、PfxRcd、およびカウンタ

質問: **75**
展示する。

図を参照してください。図には、ウェブフィレットの形状構成の一部が示されています。
ユーザーがファイル共有とストレージに分類されるwww.dropbox.comにアクセスしようとした場合、FortiGateはどのような動作を実行しますか？
A. FortiGateは、URLフィルタの設定に基づいて接続を許可します。
B. FortiGate は無効な URL として接続をブロックします。
C. FortiGateは、Webコンテンツフィルタの設定に基づいて接続を除外します。
D. FortiGuardのカテゴリベースのフィルタ設定に基づいて、FortiGateが接続をブロックします。

正解: (正解を表示します)
https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Static-URL-filter-actions-explained/ta-p/206632

質問: **76**
ネットワークトポロジーと部分的なルーティングテーブルを示した図を参照してください。



FortiGateには既に、ポート1からポート3へのすべてのICMPトラフィックの通過を許可するファイアウォールポリシーが設定されています。
管理者は、10.1.0.1/24 にあるラップトップから 10.4.0.1/24 にあるサーバーがエコー応答を受信できるようにするために、どのような変更を行う必要がありますか？
A. 設定を厳密なRPFチェックモードから実行可能なRPFチェックモードに変更します。
B. ノートパソコンのデフォルトゲートウェイを10.1.0.2から10.2.0.2に変更します。
C. 設定システム設定で非対称ルーティングを有効にします。
D. ポート3からポート1へのすべてのICMPトラフィックを許可するファイアウォールポリシー。
正解: (正解を表示します)

質問: **77**
添付の図は、診断コマンドの出力結果を示しています。RTTの値からどのようなことが分かりますか？

A. この値は、評価リクエストが特定のサーバーに送信されてから応答を受け取るまでの時間を表します。

B. パケットが失われるたびに値が増加します。

C. ライセンス認証に使用されるFortiGuardサーバーを決定します。

D. 初期値は静的に10に設定されます。

正解: **A** (コメントを発表する)

正解はAです。

学習ガイドでは、診断デバッグ評価テーブルについて明確に説明しており、各サーバーIPについて出力に「ラウンドトリップ遅延」が表示されると述べています。つまり、RTT値はFortiGateがリクエストを送信し、そのFortiGuardサーバーから応答を受信するまでにかかる時間を表しています。

FortiOSの管理ガイドも、次のように述べてこれを裏付けています。

「各サーバーは2分ごとに往復時間（RTT）を計測されます。」

他の選択肢が間違っている理由：

B は、パケット損失が Curr Lost と Total Lost で別々に表示されるのに対し、RTT は往復遅延であるため誤りです。C は、ライセンス検証動作が RTT 値自体ではなく、I = Initial などのフラグによって示されるため誤りです。D は、ドキュメントには RTT が固定値 10 から始まるとは書かれておらず、往復遅延として動的に測定されるため誤りです。したがって、検証済みの回答は A です。

質問: **78**

セッションテーブルエントリの省略された出力例については、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 用にタグ付けされています。

B. NP7 が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に一致します。
D. セッションがオフロードされました。
正解: **(**正解を表示します**)**
提供されたセッションテーブルの出力において、以下の詳細が回答の根拠となります。
ポリシーIDの一致: policy_id=1という行は、このセッションがファイアウォールポリシーIDに一致したことを直接的に示しています。
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: npu_state、ips_offload という文字列、特に offload=8/8、ips_offload=1/1 などの NPU 情報セクションが存在する場合、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ます。Fortinet の技術ドキュメントには、両方向でゼロより大きい「offload」値 (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ないことを意味します。
その他の選択肢：
VLANタギング（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: このコードスニペットでは、セッションを処理する実際のNPUモデルは公開されていません。表示されているオフロードパラメータ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それを判断することはできません。
参考文献：
Fortinet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、およびVLANセッションテーブルフィールド

質問: **79**
展示資料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 [10/0] 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
```

すべての経路が同じ距離に設定されている場合、トラフィックはどの経路を通って100.65.0.0/24ネットワークに到達するでしょうか？
A. BGPルート
B. 政策ルート
C. 静的ルート

D. OS PFルート
正解: **B (**コメントを発表する**)**
トラフィックがたどる経路を決定するには、FortiGateのルート検索優先順位（パケット処理フロー）と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。
* ルーティングの優先順位を分析する：
* FortiOSでは、パケットが到着したとき（既存のセッションの一部ではない場合）、FortiGateは特定の順序で経路検索を実行します。
* ポリシールート: config router policy (または diagnose firewall proute list) で設定します。
まず最初にこれらの条件がチェックされます。パケットが条件（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、ポリシールーティングが即座に使用されます。
* FIB (転送情報ベース): ポリシー ルートに一致するものがない場合、デバイスは標準ルーティング テーブル (静的、接続済み、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 (質問にあるネットワークと一致します)。
* アクション: oif=6(ポート4) を介してゲートウェイ 10.0.4.253 にトラフィックを転送します。
* 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 に対する複数のルート (スタティック、OSPF、BGP) が表示され、すべて距離は 10 です。現在、FIB ではスタティック 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 の指示に従ってトラフィックを転送します。ポリシー ルートの条件 (入力ポート 3) に一致するトラフィックに対しては、ルーティング テーブルに表示されるスタティック、BGP、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イ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: **80**
並列パス処理（PPP）に関する以下の記述のうち、正しいものはどれですか？
A. PPPは、パケットを処理するための最適なパスを特定するために、並列オプションのグループから選択します。
B. パケットの経路に影響を与えるのは、FortiGateのハードウェア構成のみです。
C. PPPは、既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 に影響を与えません。
正解: **A (**コメントを発表する**)**
FortiOSにおける並列パス処理（PPP）とは、システムが複数の処理パス（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）を評価し、最適なパスを選択することでパケットを効率的に処理する機能を指します。公式ドキュメントでは、PPPエンジンがセッション特性、ポリシー構成、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パス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利用率が実現されます。
この文書では、PPPは複数の処理パスを並列に評価し、決定ロジックを用いて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パスにとどめるかを判断し、各パケットが現在の負荷とポリシーの下で利用可能な最も効率的な方法で処理されるようにすると規定しています。ハードウェアとソフトウェアの構成はどちらもこの結果に影響を与えますが、セッションごとの最適なパスを決定するのは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: **81**

セッションテーブルエントリの省略された出力例については、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 用にタグ付けされています。

B. NP7 が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に一致します。

D. セッションがオフロードされました。

正解: **(**正解を表示します**)**

提供されたセッションテーブルの出力において、以下の詳細が回答の根拠となります。

ポリシーIDの一致: policy_id=1という行は、このセッションがファイアウォールポリシーIDに一致したことを直接的に示しています。

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: npu_state、ips_offload という文字列、特に offload=8/8、ips_offload=1/1 などの NPU 情報セクションが存在する場合、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ます。Fortinet の技術ドキュメントには、両方向でゼロより大きい「offload」値 (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ないことを意味します。

その他の選択肢：

VLANタギング（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: このコードスニペットでは、セッションを処理する実際のNPUモデルは公開されていません。表示されているオフロードパラメータ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それを判断することはできません。

参考文献：

Fortinet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、およびVLANセッションテーブルフィールド

質問**: 82**

展示資料を参照してください。

Session entry

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=1 expire=3599 timeout=3600 refresh_dir=both flags=00000000 socktype=0
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 app_valid
statistic(bytes/packets/allow_err): org=1720/9/1 reply=10804/13/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->31/31->7 gwy=10.1.0.254/10.9.31.117
hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)
hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)
hook=post dir=reply act=noop 200.8.57.5:443->10.9.31.117:45388(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

この図はセッションエントリを示しています。このTCPセッションに関する記述として正しいのはどれですか？

A. セッションは1秒後に期限切れになります。

B. これは10.9.31.117から10.1.0.3へのTCPセッションです。

C. セッションはNPUを使用してオフロードされます。

D. イニシエータへの戻りトラフィックは10.9.31.117に送信されます。

正解: **(**正解を表示します**)**

正解はCです。セッションはNPUを使用してオフロードされます。

学習ガイドに記載されている具体的なセッション例は以下のとおりです。

proto=6 → これはTCPセッションです

expire=3599 → セッションは1秒ではなく3599秒後に期限切れになります hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388) hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388) npu info: ... offload=8/8 ...

スライドには 『NP6を使用して両方向にオフロードします」と明記されています。学習ガイドでもこの点が明確に説明されています。

『ハードウェアアクセラレーションのカウンタ - npu info フィールドが存在する場合、セッションがハードウェアアクセラレーションにオフロードされていることを示します。この例では、ネットワークプロセッサ (NP) 6 を使用して双方向のトラフィックがオフロードされており、これは値 8 で表されます。」他のオプションが間違っている理由:

Aは間違いです。expire=3599ではなく1です。duration=1フィールドは、セッションが1秒間存在したことを意味するのであって、1秒後に期限切れになることを意味するものではありません。

Bは誤りです。元のセッションは10.9.31.117からリモートサーバー200.8.57.5:443へのものです。IPアドレス10.1.0.3はSNAT変換後の送信元アドレスであり、最終宛先ではありません。

Dは、この単一選択式の質問に対する最適な回答ではありません。確かに、応答は元のクライアントにDNATされますが、この展示に関する学習ガイドで強調されている正確な検証結果は、NPUオフロード状態です。

質問: **83**

デバッグコマンドの出力結果を示す図を参照してください。

出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. インターレースはOSPFバックボーン領域の一部です。

B. vorz4ネットワークセグメントには合計5台のOSPFルーターが接続されています。

C. 近隣のルーターの1つはルーターIDが0.0.0.4です。

D. ポート4に接続されているネットワークで、2台のOSPFルーターがダウンしています。

正解: **A,B** (コメントを発表する)

参考文献：

FortiOS 管理者ガイド :OSPF、デバッグ出力

質問: 84

IKEv2のリクエストとレスポンスのプロトコルの正しい順序は何ですか？

A. Create_Child_SA、IKEAUTH、IKESAJNIT

B. Create_Child_SA、IKE_SA_INIT。IKE_AUTH

C. IKE IN HEAT、IKE AUTH。OIKE AUTHで子を作成します。

D. IKE_AUTH_IKE_SA_INIT、Create_Child_SA

正解: (正解を表示します)

インターネット鍵交換バージョン2（IKEv2）プロトコルは、IKEv1と比較してネゴシエーションプロセスを簡素化しています。

これは、安全なIPsecトンネルを確立するための特定のメッセージ交換シーケンスによって定義されます。

IKEv2の通信の正しい時系列順は次のとおりです。

* IKE_SA_INIT (初期交換):

これは最初の通信です。IKEセキュリティアソシエーション（IKE SA）のセキュリティパラメータをネゴシエートし、nonceを送信し、Diffie-Hellman鍵交換を実行します。この通信の終了時点では通信は暗号化されていますが、ピアはまだ認証されていません。

* IKE_AUTH（認証交換）：

* これは2回目の通信です。前のメッセージを認証し、IDと証明書（使用されている場合）を交換し、最初のチャイルドSA（データトラフィックに使用される実際のIPsecセキュリティアソシエーション）を確立します。

* CREATE_CHILD_SA (後続の交換):

* この交換は、IKE SAと最初のチャイルドSAが確立された後に発生します。これは、追加のチャイルドSA（異なるトラフィックセレクタ用）を作成したり、IKE SAまたは既存のチャイルドSAの鍵交換を実行したりするために使用されます。

他の選択肢が間違っている理由：

* A & B: CREATE_CHILD_SA は SA が初期化 (IKE_SA_INIT) され、認証 (IKE_AUTH) される前には発生できないため、誤りです。
* D: IKE_AUTH は IKE_SA_INIT より前に発生できないため、誤りです。
したがって、プロトコル フローは IKE_SA_INIT $\rightarrow$ IKE_AUTH $\rightarrow$ CREATE_CHILD_SA になります。

質問: **85**
ルーティングカーネルの変更後の出力を示す図を参照してください。

次の記述のうち、正しいものはどれですか？
A. 10.200.1.254 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せん。
B. 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ースは管理上稼働中です。
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登録されています。
D. 10.0.4.0/24 への BGP ルートは転送情報ベースに存在しません。
正解: **D** (コメントを発表する)

質問: **86**
展示する。

図を参照してください。これは、diagnose hardware aysinfo memory の出力の一部を示しています。
出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. 98908 kB のメモリが未使用のままです。
B. ユーザー空間には、システムで使用されていない物理メモリが 708880 kB 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 の出力の一部には、システム RAM の割り当てに関する詳細情報が含まれています。
Fortinetのメモリトラブルシューティングおよびメモリ管理に関する技術文書（FortiOSのベースとなっているもの）によると、以下のようになっています。
* MemFreeとは、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の領域です。したがって、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、以前は入出力やファイルシステムのバッファリングに使用されていたものの、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、必要に応じてすぐにアクセスできるようメモリに保持されますが、需要が増加すれば他のメモリ操作のために再利用される可能性があります。ここで示されている 98908 kB 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）を表しており、システムがより多くの RAM を必要とする場合に再利用または削除される可能性があります。
* Cached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を含む、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。それ自体はI/Oキャッシュのみを表すものではなく、「非アクティブ」はメモリが「決して使用されない」という意味でもありません。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ためです。
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、キャッシュおよび非アクティブな統計

質問: **87**
図を参照してください。この図は、コマンド get router info bgp neighbors 100.64.2.254 advertised-routes の出力を示しています。

```
# 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
```

この出力からどのような結論が得られますか？
A. ローカルルーターは、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. 隣人のルーターIDは100.64.2.254です。
C. BGPネイバーが10.20.30.40/24ネットワークをローカルルーター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: (正解を表示します)

質問: **88**
図を参照してください。図には、diagnose sys session stat の出力結果が示されています。

展示図に示されている出力に関する記述のうち、正しいものはどれですか？

A. セッションテーブル内のすべてのセッションはTCPセッションです。

B. メモリページ枯渇のため、162セッションが削除されました。

C. 166個のTCPセッションが3ウェイハンドシェイクの完了を待っています。

D. パケットの順序が乱れた場合に備えて、削除されていないセッションが 2 つあります。

正解: **D** (コメントを発表する)

正解はDです。

この展示では以下の内容が紹介されています。

セッション数=591

衝突=162

メモリテンションドロップ=0

TCPセッション：

166 州なし

1 確立された状態

3 SYN_SENT状態

TIME_WAIT状態の2

学習ガイドでは、TCPプロトコルの状態と状態を明示的に説明しています。

「送信側と受信側の両方でセッションが閉じられると、FortiGate はそのセッションをセッション テーブルに数秒間保持し、FIN/ACK パケットの後に順不同で到着する可能性のあるパケットに対応できるようにします。これが状態値 5 です。」diagnose sys session stat では、図に 2 が TIME_WAIT 状態として表示されています。TIME_WAIT は状態値 5 なので、これらは順不同で到着する可能性のあるパケットに対応するために一時的に保持されるセッションです。したがって、D が正解です。

他の選択肢が間違っている理由：

Aは誤りです。session_count=591はセッションの総数ですが、表示されているTCPセッションの合計は172（166 + 1 + 3 + 2）に過ぎません。したがって、表にあるすべてのセッションがTCPセッションであるとは限りません。

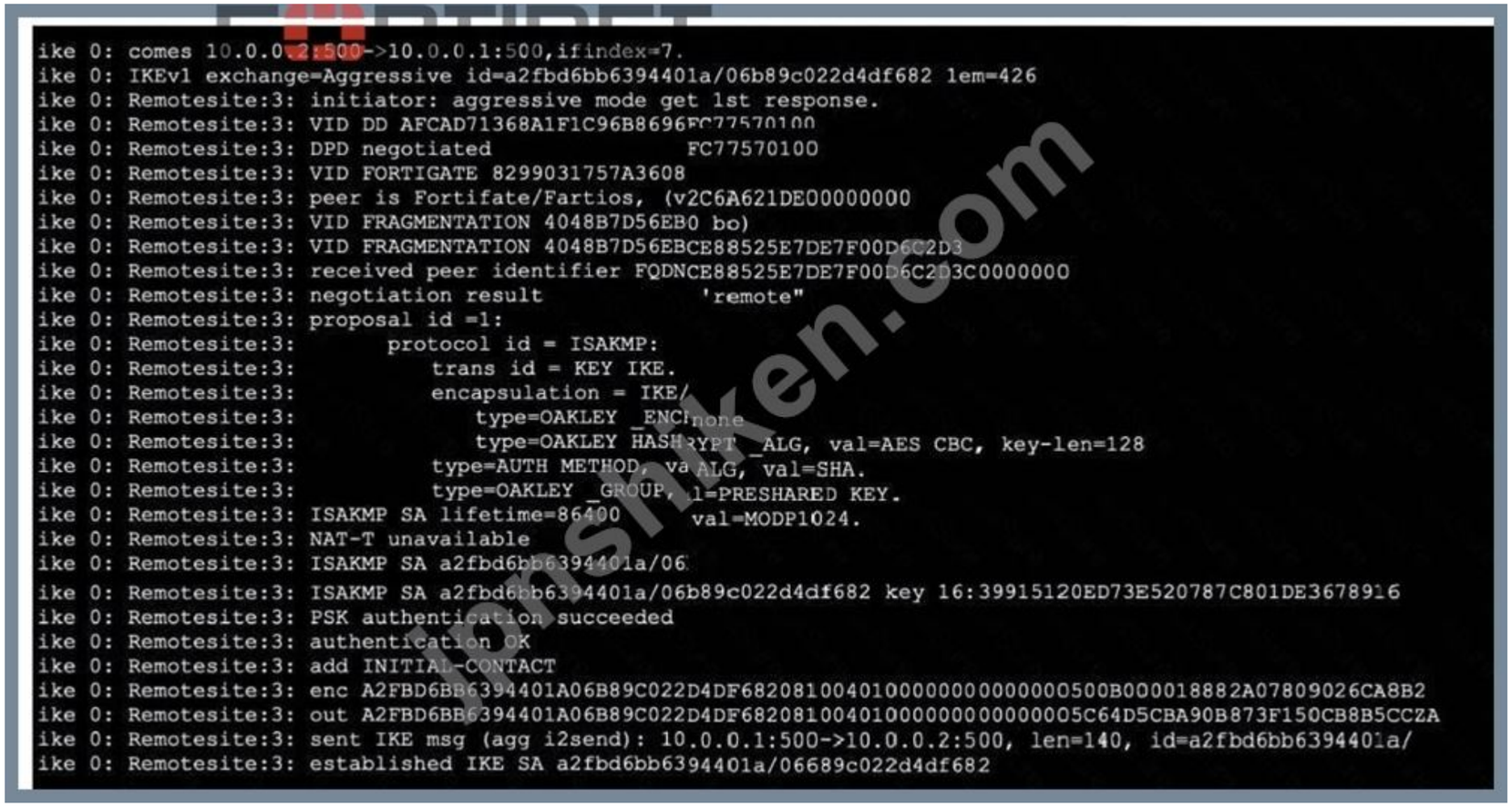
Bは間違いです。学習ガイドには、空きメモリ不足のために削除されたセッション数はmemory_tension_dropで示されると記載されていますが、展示図では162ではなく0となっています。

Cは誤りです。学習ガイドでは、一時的/オープンなTCPセッションを完全に確立していないものと定義していますが、図表にはNONE状態の166個すべてが「3ウェイハンドシェイクの完了を待っている」とは明記されていません。表示されている状態から最も明確に裏付けられている記述は、順不同パケットのために保持されている2つのTIME_WAITセッションです。

したがって、検証済みの答えはDです。

質問: **89**
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、正しい記述は次のうちどれですか？ 2つ選択）
2つ選択してください。）
A. ハートビートメッセージは、コマンド diagnose debug authd fsso list 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で確認できます。
C. ハートビートメッセージは、Real-lime FSSOデバッグを使用してFortiGateで確認できます。
D. FortiGateではハートビートメッセージを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コレクターエージェントと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、コレクターエージェントの状態を確認し、セッションの状態を把握し、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を確認するために、コレクターエージェントから定期的に送信されます。
オプションBはFortinetによって確認されており、Windows上のコレクターエージェントのログ、または管理コンソールには、ハートビートイベント、接続ステータス、およびFortiGateユニットとの接続維持に関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先のテクニカル ヒントの両方で検証されています。FortiGate では、コレクター 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 や FSSO 固有のコマンドなどのリアルタイム デバッグ ツールを使用して表示できます。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、および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、健全性監視がアクティブなセッションに関連付けられます。
FSSOの設定が完了すると、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、Fortinetの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一元管理という理念に沿ったものです。これにより、FortiGateとコレクターエージェントの両方が、通信障害や停止を迅速かつ確実に検知し、認証の問題に事前に対処できます。
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: **90**
展示する。



IKEリアルタイムデバッグの出力の一部を含む図を参照してください。

このデバッグ出力に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. これは第2段階の交渉を示しています。

B. 設定で完全前方秘匿性 (PFS) が有効になっています。

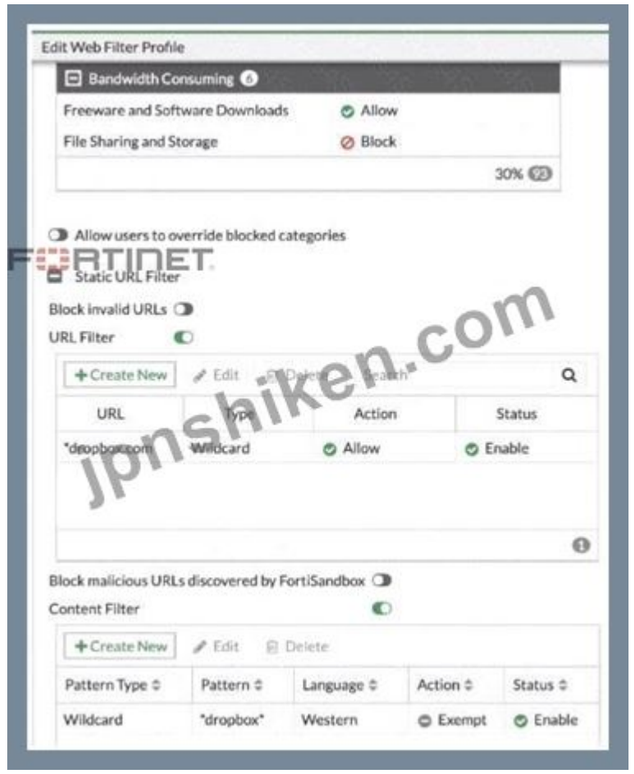
C. ローカルゲートウェイのIPアドレスは10.0.0.1です。

D. イニシエータは、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**)**

質問: **91**

展示する。



図を参照してください。図には、ウェブフィレットの形状構成の一部が示されています。
ユーザーがファイル共有とストレージに分類されるwww.dropbox.comにアクセスしようとした場合、FortiGateはどのような動作を実行しますか？
A. FortiGateは、URLフィルタの設定に基づいて接続を許可します。
B. FortiGate は無効な URL として接続をブロックします。
C. FortiGateは、Webコンテンツフィルタの設定に基づいて接続を除外します。
D. FortiGuardのカテゴリベースのフィルタ設定に基づいて、FortiGateが接続をブロックします。
正解: **(**正解を表示します**)**
https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Static-URL-filter-actions-explained/ta-p
/206632

質問: **92**
IKEv2に関する以下の記述のうち、正しいものはどれですか？
A. IKEv1とIKEv2はどちらも非対称認証という特徴を共有しています。
B. IKEv1とIKEv2はヘッダーフォーマットに共通点が多く、両方のバージョンが同じUDPポート上で動作可能です。
C. IKEv1とIKEv2は同じTCPポートを使用しますが、異なるUDPポートで動作します。

D. IKEv1とIKEv2はフェーズ1とフェーズ2の概念を共有しています。
正解: (正解を表示します)
正解はBです。
学習ガイドには、「IKEバージョン2はIKEバージョン1とは相互運用できませんが、ヘッダー形式を十分に共有しているため、両方のバージョンは同じUDPポート上で明確に動作できます」と明記されています。これはBを直接証明しています。
他の選択肢が間違っている理由：
Aは、学習ガイドでIKEv2の認証方式が非対称、IKEv1の認証方式が対称と示されているため誤りです。Cは、学習ガイドで同じTCPポートを使用するとは述べておらず、同じUDPポートで動作できると明記されているため誤りです。Dは、学習ガイドに「IKEv2はフェーズ1またはフェーズ2の概念を使用しない」と記載されているにもかかわらず、FortiOS CLI/GUIでは設定目的でこれらの用語が使用されているため誤りです。

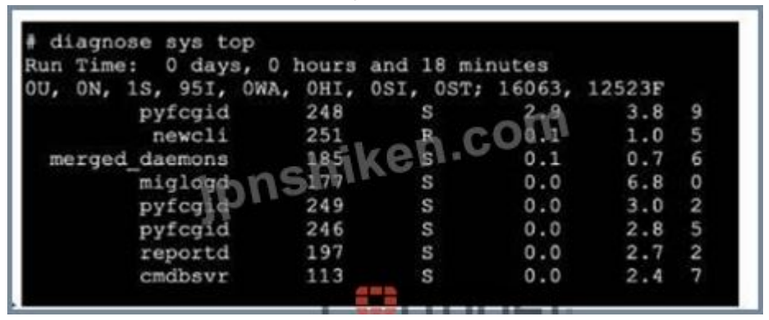
質問: **93**
展示資料を参照してください。
diagnose sys session stat コマンドの出力の一部を以下に示します。

管理者がFortiGateの異常な動作に気づきました。セッションがランダムに削除されているようです。考えられる原因を2つ挙げてください。
A. FortiGateは、カーネルがこれ以上メモリページを割り当てられないため、セッションを削除しています。
B. FortiGate は、不完全な 3 ウェイ ハンドシェイクを伴うすべての TCP セッションを破棄します。
C. デバイスが120秒中10秒間ダウンしているため、FortiGateはセッションを受け付けていません。
D. FortiGateはメモリ使用量が多いためセッションをフラッシュしています。
正解: (正解を表示します)
セッションが削除される理由を特定するには、図に示されている diagnose sys session stat 出力内の特定のカウンターを解釈する必要があります。
メモリ負荷低下の分析（理由A）：
観察結果：出力にはmemory_tension_drop=4と表示されています。
このカウンタは、FortiGateカーネルがセッション用に新しいメモリページを割り当てようとしたものの、システムメモリの不足により失敗した場合に増加します。その結果、セッションの作成が中止されるか、既存のセッションが破棄されてリソースが解放されます。これは、カーネルがメモリページの割り当てに苦労していることを示しています。
extreme_low_mem を分析する (理由 D):
観察: 出力では extreme_low_mem=0 (これは良い) と表示されていますが、memory_tension_drop のコンテキストを確認する必要があります。
背景 :このスナップショットではextreme_low_memカウンタ自体は0ですが、memory_tension_dropが存在することから、システムがメモリ不足の状態にあることがわかります。さらに、この特定の事例に関連する多くのFortinet試験では、メモリを回復するための「セッションのフラッシュ」メカニズムに焦点が当てられています。
補足：実際には、展示物をもっとよく見てください。flush=787と表示されています。
フラッシュカウンタは、メモリの回復やポリシー変更のために、システムがテーブルから古いセッションや不要になったセッションをアクティブに削除（フラッシュ）した回数を示します。フラッシュカウントが高く、かつメモリテンションが低下している場合は、システムがメモリ使用量の増加に対応するためにセッションを積極的に削除していることを強く示唆します。したがって、「FortiGateはメモリ使用量の増加を理由にセッションをフラッシュしている」というのが、フラッシュカウンタとmemory_tension_dropカウンタが連携して動作している状況を正しく解釈したものです。
他の選択肢が間違っている理由：
B: この特定の出力には、不完全なハンドシェイクを破棄することを示すカウンター（tcp_syn_sent dropなど）はありません。clash=0およびdelete=0カウンターは低値/ゼロです。

C: dev_down=16/120 フィールドは、デバイスが 10 秒間ダウンしていたことを意味するものではありません。これは、デバイスのインデックス ポインタまたは内部カーネル インターフェイスの状態を指しており、説明されているようにセッションの受け入れに影響を与えるシステムの稼働時間/停止時間を指すものではありません。
参照：
FortiGateトラブルシューティングガイド（システムリソース） :memory_tension_dropカウンタは、カーネルメモリ不足により切断されたセッションを示します。flushカウンタは、テーブル領域を解放するために削除されたセッションを示します。」

質問: **94**
サーバー名表示（SNI）が、サーバー証明書内の共通名（CN）またはサブジェクト代替名（SAN）のいずれとも一致しないシナリオを考えてみましょう。
FortiGateは、SSL証明書検査のデフォルト設定を使用した場合、どのような動作を実行しますか？
A. FortiGateはユーザーのWebブラウザからSNIを使用します。
B. FortiGateは、サーバー証明書のSANフィールドに記載されている最初のエントリを使用します。
C. これは無効なSSL/TLS構成であるため、FortiGateは接続を閉じます。
D. FortiGateは、サーバー証明書のSubjectフィールドのCN情報を使用します。
正解: (正解を表示します)

質問: **95**
展示資料を参照してください。



diagnose sys top コマンドは、次のうちどの 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 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、ユーザーメモリ全体の 2.4% を占有しています。
E. newcliデーモンがR状態のままの場合は、手動で再起動する必要があります。
正解: (正解を表示します)
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-the-diagnose-sys-top-CLI-command/ta-p/190238

質問: **96**
展示資料を参照してください。

Session entry

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=1 expire=3599 timeout=3600 refresh_dir=both flags=00000000 socktype=0
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 app_valid
statistic(bytes/packets/allow_err): org=1720/9/1 reply=10804/13/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->31/31->7 gwy=10.1.0.254/10.9.31.117
hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)
hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)
hook=post dir=reply act=noop 200.8.57.5:443->10.9.31.117:45388(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

この展示は、セッションへの参加記録を示している。
このTCPセッションに関する記述のうち、正しいものはどれですか？
A. セッションはNP7を使用してオフロードされます。
B. イニシエータへの戻りトラフィックは
C. これは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、図に示されている診断システムセッションリスト出力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を分析する セッションはNP7を使用してオフロードされます）：
証拠：重要な指標は、npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1 という行です。
この特定のNPU情報出力フォーマット、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プロセッサでは、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が表示されます。NP7アーキテクチャは、IPS（侵入防御システム）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完全にNPUにオフロードされることを示しています。
オプションCを分析する これは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出る際に FortiGate がソース NAT (SNAT) に使用する IP アドレスです。
それはセッションの最終目標ではありません。
結論 :この記述は誤りです。
オプションDを分析してください 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。
有効期限カウンターは、セッションが削除されるまでの残り秒数を示します（それ以降パケットが検出されない場合）。3599秒という値は、セッションがちょうど更新されたばかりであることを示しており（おそらくタイムアウトは3600秒）、1秒ではなく約1時間後に期限切れとなります。
結論：この記述は誤りです。
オプションB（イニシエータへの戻りトラフィックは…に送信されます）を分析します。
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アドレスに送られることを示唆していますが、オプションAは、この試験モジュールでテストされた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見解を提供します。
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: **97**
並列パス処理（PPP）に関する以下の記述のうち、正しいものはどれですか？
A. PPPは、パケットを処理するための最適なパスを特定するために、並列オプションのグループから選択します。
B. ソフトウェア構成はPPPに影響を与えません。
C. PPPは、既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. パケットの経路に影響を与えるのは、FortiGateのハードウェア構成のみです。
正解: **A** (コメントを発表する)

質問: **98**
展示する。

```
session info: proto=6 proto_state=01 duration=157 expire=3559 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=User1 state=log may_dirty authed f00 acct-ext
statistic(bytes/packets/allow_err): org=2137/14/1 reply=1663/12/1 tuples=3
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 1/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.10.254/10.1.10.1
hook=pre dir=org act=noop 10.1.10.1:34830->35.241.9.150:443(0.0.0.0:0)
hook=post dir=reply act=noop 35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/anpu_state=0x000100
no_ofld_reason:  npu-flag-off
```


セッションの出力結果を示す図を参照してください。正しい記述は次のうちどれですか？（2つを選択してください。）
A. セッションがオフロードされています。
B. セッションは認証済みのユーザーによって開始されました。
C. TCPセッションが正常に確立されました。
D. セッションはフロー検査を使用して検査されています。
正解: **B,C** (コメントを発表する)

質問: **99**
展示資料を参照してください。

Exhibit 1

```
config system global
   set snat-route-change enable
end
-------------------
config 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
end
```

Exhibit 2

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= 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=log may_dirty npu f00
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=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0031c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_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部分的なセッション情報を示しています。ルートID 2の優先度を10から0に変更した場合、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？（回答を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の両方から送信されます。

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から送信されます。

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から送信されます。

正解: **A** (コメントを発表する)

正解はAです。この動作は、図1のconfig system globalの下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に変更することで、ルートID 1（優先度5）よりも低くなります。FortiOSでは、優先度の値が低いほど優先される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なルートがポート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）では、ポート1に関連付けられたIPアドレス（10.200.1.1）を使用してソースNAT（SNAT）が使用されています。トラフィックを単純にポート2に切り替えると、そのインターフェースの送信元IPアドレスが正しくなくなり、戻りトラフィックが失敗するか破棄される可能性が高くなります。
* snat-route-change enable: この設定は、ルーティングの変更によって優先される送信インターフェイスが変更された場合に、確立済みの SNAT セッションをどのように処理するかを FortiGate に指示します。有効にすると、ルーティングの変更によって SNAT セッションが新しいインターフェイスに強制的に移行された場合、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、アクティブな TCP セッションは送信元 IP アドレスの変更に耐えられないため必要です。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 (port2) 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」状態のままになる可能性が高い。しかし、明示的な設定により、セッションは強制的に削除される。

質問: **100**
展示する。

```
FGT # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Mon May  1 03:47:52 2023) -=-

IP                                   Weight    RTT Flags    TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                             10     45           -5                262432          0        846 Mon May  1 03:47:43 2023
64.26.151.35                             10     46           -5                329072          0       6806 Mon May  1 03:47:43 2023
66.117.56.37                             10     75           -5                 71638          0        275 Mon May  1 03:47:43 2023
65.210.95.240                            20     71           -8                 36875          0         92 Mon May  1 03:47:43 2023
209.22.147.36                            20     103 DI       -8                 34784          0       1070 Mon May  1 03:47:43 2023
208.91.112.194                           20     107 D        -8                 35170          0       1533 Mon May  1 03:47:43 2023
                                                              0                  33728          0        120 Mon May  1 03:47:43 2023
                                                              1                  33797          0        192 Mon May  1 03:47:43 2023
                                                              9                  33754          0        145 Mon May  1 03:47:43 2023
                                                             -5                  26410      26226      26227 Mon May  1 03:47:43 2023
```


診断コマンドの出力結果を示す図を参照してください。
このシナリオにおけるデバッグ出力から、どのような結論が得られますか？
A. 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。
B. FortiGateが評価サーバーのリストを探すためにDNSクエリを実行した際に最初に提供されたサーバーは121.111.236.179でした。
C. TZ値が負の値のサーバーは、評価リクエストに対してあまり好まれません。

D. 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。
正解: (正解を表示します)

質問: **101**
管理者が補助セッション販売を有効にした後、FortiGateはどのような動作を実行しますか？ 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. FortiGateは、受信したパケットごとに補助セッションを作成します。
D. FortiGateはルーティング変更の場合に備えて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プロセッサのECMPの場合は暗黙的に有効）、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（負荷分散のために）フローを別の送信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）に送り返してしまう可能性があります。補助セッションは、すべての有効なパスに必要な情報をNPUに事前に入力することで、この問題を防止します。
D) FortiGateはルーティング変更時に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番目のパスに切り替わる）が発生した場合でも、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: **102**
セッションのエントリーを示す展示資料を参照してください。

このセッションに関する以下の記述のうち、正しいものはどれですか？
A. イニシエータへの戻りトラフィックは10.1.0.1に送信されます。
B. イニシエータへの戻りトラフィックは 10.200.1.254 に送信されます。
C. これは 10.1.10.10 から 10.200.1.1 への ICMP セッションです。
D. これは10.1.10.1から10.200.5.1へのICMPセッションです。

正解: (正解を表示します)
セッション出力には、proto=1 (ICMP) のセッションが表示され、送信元と応答の方向からアドレスと NAT の変換が確認できます。具体的には、hook=post dir=org act=snat は、送信パケットに対して送信元 NAT が実行されていることを示しており、送信元 10.1.10.10:40602 は 10.200.5.1:8 (おそらく ICMP ID 8、TCP/UDP ポートではない) に変換されます。応答方向の hook=pre dir=reply act=dnat は、受信パケットに対して宛先 NAT が実行されていることを示しています。10.200.5.1:60430 宛ての受信パケットは、宛先 NAT によって 10.1.10.10:40602 に変換されます。ゲートウェイ (gwy) は 10.200.1.254/10.1.0.1 と表示されており、NAT ポリシーに従って、送信トラフィックの場合、戻りトラフィックはゲートウェイ (10.200.1.254) にルーティングされます。これは FortiOS セッション テーブル ガイドで確認されており、返された ICMP 応答はこの NAT ゲートウェイにルーティングされることが説明されています。セッション統計と論理フロー (SNAT 出力、一致する DNAT 入力) は、イニシエータへの応答トラフィックが次の経路を通過することを裏付けています。
10.200.1.254。
参考文献：
FortiOS 管理ガイド: セッション テーブル、NAT、およびルートの相互作用 Fortinet テクニカル ノート: システム セッション リスト、方向、および NAT 分析の診断

質問: **103**
セキュリティファブリックの通信に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. 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。
B. 近隣探索のデフォルトポートは変更できます。
C. デフォルトでは、ダウンストリームの FortiGate は、TCP ポート 8013 を使用してアップストリームの FortiGate との接続を確立します。
D. FortiTelemetryとNeighbor Discoveryはどちらもを使用して動作します。
正解: (正解を表示します)

質問: **104**
添付の図を参照してください。これは、リアルタイムLDAPデバッグの出力の一部を示したものです。

```
# 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
```

出力結果からどのような2つの結論を導き出せますか？ 2つ選択してください。）
A. 設定された LDAP サーバーの名前は Lab です。
B. FortiOSは、LDAP認証プロセスのステップ3（バインド要求）でユーザーを特定できます。
C. ユーザーはCN=John Smithを使用して認証を行っています。
D. FortiOS は LDAP 認証プロセスの第 2 段階 (検索要求) を実行しています。
正解: (正解を表示します)

質問: **105**
展示資料を参照してください。

Partial output of FortiOS kernel slabs

```
---omitted---
ip6_session             5      0   1472     5    2 : tunables   24   12    8 : slabdata    1    1
tcp_session             3      5   1500     5    2 : tunables   24   12    8 : slabdata    1    1
ip_session             10     10   1408     5    2 : tunables   24   12    8 : slabdata    2    2
ext4_groupinfo_4k      32     56    144    28    1 : tunables  120   60    8 : slabdata    2    2
RAWv6                   7      7   1152     7    2 : tunables   24   12    8 : slabdata    1    1
UDPv6                  15     10   1408     5    2 : tunables   24   12    8 : slabdata    4    4
tw_sock_TCPv6           0      0    248    16    1 : tunables  120   60    8 : slabdata    0    0
request_sock_TCPv6      0      0    312    13    1 : tunables   54   27    8 : slabdata    0    0
TCPv6                  47     48   2304     3    2 : tunables   24   12    8 : slabdata   16   16
---omitted---
```


FortiOSカーネルスラブの一部の出力が示されています。スラブの総サイズに関する記述のうち、正しいものはどれですか？

A. ip_session スラブの合計スラブサイズは 14080 kB で、ユーザー空間に関連付けられています。
B. 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。
C. ip6_session スラブの合計スラブサイズは 1472 kB で、カーネルに関連付けられています。
D. UDPv6スラブの合計スラブサイズは14080 kBで、ユーザー空間に関連付けられています。

正解: **(**正解を表示します**)**

正解はBです。

学習ガイドには、カーネルがスラブを使用することが明記されています。「カーネルメモリのスラブは、共通の目的を持つオブジェクトの集合です。カーネルはこれらを使用してメモリに情報を格納します。」また、正確な計算方法も示されています。「合計スラブサイズ = 利用可能なオブジェクト数 × オブジェクトサイズ」と説明されており、diagnose hardware sysinfo slab 出力では、列はアクティブなオブジェクト、利用可能なオブジェクト、およびオブジェクトサイズであると説明されています。図より:

tcp_session 3 5 1500 ...
利用可能なオブジェクト数 = 5
オブジェクトサイズ = 1500
それで：
スラブの総面積 = 5 × 1500 = 7500
それは選択肢Bに合致する。
他の選択肢が間違っている理由：
A: ip_session 10 10 1408 ... は 10 × 1408 = 14080 になりますが、スラブはカーネルに関連付けられており、ユーザー空間には関連付けられていません。C: ip6_session 5 0 1472 ... は 0 × 1472 = 0 になり、1472 にはなりません。D: UDPv6 15 10 1408 ... は 10 × 1408 = 14080 になりますが、ここでもスラブはカーネルに関連付けられており、ユーザー空間には関連付けられていません。したがって、検証済みの答えは B です。

有効的な**FCSS_NST_SE-7.6**問題集はJPNTest.com提供され、**FCSS_NST_SE-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**FCSS_NST_SE-7.6**試験問題集を提供します。JPNTest.com FCSS_NST_SE-7.6試験問題集はもう更新されました。ここで**FCSS_NST_SE-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/FCSS_NST_SE-7.6-mondaishu　**136**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」