Fortinet.FCSS_NST_SE-7.4.v2026-06-26.q63

試験コード：	FCSS_NST_SE-7.4
試験名称：	FCSS - Network Security 7.4 Support Engineer
認証ベンダー：	Fortinet
無料問題の数：	63
バージョン：	v2026-06-26
ページの閲覧量：	102
問題集の閲覧量：	632

https://www.jpnshiken.com/shiken/Fortinet.FCSS_NST_SE-7.4.v2026-06-26.q63.html

質問: **1**
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. ソフトウェア構成は PPP に影響を与えません。
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、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。
D. 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。
正解: **C** (コメントを発表する)

質問: **2**
証拠資料 1。

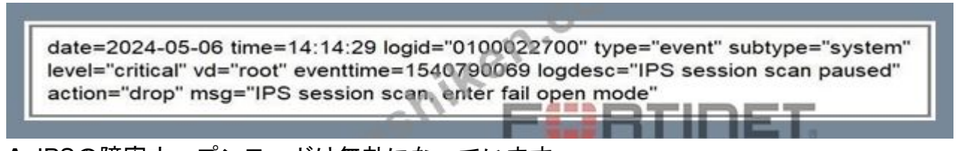
```
config system global
    set snat-route-change disable
end
-----------------
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    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. set snat-route-change enable を設定します。
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. ポートの優先度を静的ルートで11に変更します。
正解: **(**正解を表示します**)**

質問: **3**
図を参照してください。イベントログに示されているように、FortiGateは省電力モードになっています。
展示資料に示されている情報に基づいて、FortiGate侵入防御システム（IPS）の構成についてどのような結論を導き出せますか？



A. IPSの障害オープンモードは無効になっています。
B. 検査対象のプロトコルはサポートされていません。
C. IPSプロファイルはプロキシベースです。
D. 新しいパケットは検査されずに通過する可能性があります。
正解: **(**正解を表示します**)**
「フェイルオープンモードに入ります」というメッセージは、メモリ負荷が高まった際にIPSがフェイルオープンするように設定されていることを示しています。そのため、メモリ節約モードが作動すると、新しいパケットは完全な検査なしで通過できるようになります。

質問: **4**
添付資料には、FortiGate上の2つのVPNの部分的な設定が含まれていますので、ご参照ください。

Exhibit 1

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

Exhibit 2

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


管理者は、2つの異なるユーザーグループ向けに2つのVPNを設定しました。Users-2グループに属するユーザーはVPNに接続できません。診断コマンドを実行した結果、FortiGateがUsers-2グループのメンバーに対してuser-2 VPNを正しく設定していないことが判明しました。
問題を解決するために、管理者はどの2つの変更を行う必要がありますか？ 2つ選択してください。）

A. 両方のVPNでXAuthを有効にする。
B. 両方のVPNで異なる事前共有キーを使用します。
C. 両方のVPNで特定のピアIDを設定します。
D. 両方のVPNで攻撃モードに変更します。
正解: **(**正解を表示します**)**

質問: **5**
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: **A,C (**コメントを発表する**)**

質問: **6**
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。

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. 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。
B. FortiGateデバイスのパスワードが一致しません。
C. 隣接関係を試みている 2 つの FortiGate デバイスは、エリア 0.0.0.0 にあります。
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: **7**
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. NP7 がこのセッションのオフロードを処理しています。
B. セッションがオフロードされました。
C. トラフィックはポリシーID 1に一致します。

D. トラフィックは VLAN 0000 用にタグ付けされています。
正解: **(**正解を表示します**)**

質問: **8**
BGPデータベースの出力結果を示す図を参照してください。

正しい記述はどれですか？ 2つ選択してください。）
A. 出力には、ローカル ルーターだけでなく、すべてのネイバーによってアドバタイズされたすべてのプレフィックスが表示されます。
B. 10.20.30.0'24 のアドバタイズされたプレフィックスは、別のルーティングプロトコルの再配布によってアドバタイズされています。
C. ネットワークコマンドを使用して、10.20.30.0'24 のアドバタイズされたプレフィックスが設定されました。
D. 最初の4つのプレフィックスは、従来のルートアドバタイズメントを使用してアドバタイズされています。
正解: **(**正解を表示します**)**

質問: **9**
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. 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。
B. FortiGateは、ユーザーがログオフした場合に備えて、ワークステーションを頻繁にポーリングします。
C. コレクターエージェントは、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。
D. FortiGate はこのイベントを TCP ポート 8000 経由でポーリングしました。
E. 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**)**
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。
エージェントレスポーリングモードでは、FSSOはドメインコントローラーのセキュリティログからKerberos TGTイベント（例4768）のみを読み取り、対応する「ログオフ」イベントがないため、ユーザーがログオフしたかどうかを確認できません。
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。

空白の workstation= フィールドとイベント ID 4768 の使用は、fssod がドメインコントローラーまたはコレクターエージェントからプッシュされたイベントを受信するのではなく、ドメインコントローラーのイベントログをポーリングしていることを示しています。

質問: **10**
添付資料を参照してください。資料には、diagnose vpn tunnellist の出力が含まれています。

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「ポート4500」
B. 診断スニファパケット「ホスト 10.0.10.10」
C. 診断スニファパケット 'ip proto 50'
D. 診断スニファパケット「esp」およびホスト10.200.3.2「
正解: **A** (コメントを発表する)

質問: **11**
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. 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。
B. 98908 kB のメモリが未使用のままです。
C. 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。
D. 641364 kBのメモリが割り当てられているI/Oキャッシュ。
正解: **B,C** (コメントを発表する)

質問: **12**
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. 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。

D. 近隣のルーターの1つはルーターIDが0.0.0.4です。

正解: **(**正解を表示します**)**

質問: **13**

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. 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。

B. 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。

C. 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。

D. miglogdデーモンはCPUコアID 0で実行されています。

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

正解: **A,B,D (**コメントを発表する**)**

質問: **14**

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 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        100     218    3220        0    0    0 never     Connect

Total number of neighbors 1
```

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. ローカルルーターがネイバーからキープアライブメッセージを受信していません。

B. BGPネイバーへのアクティブなルートがありません。

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. 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ませんでした。

正解: **(**正解を表示します**)**

BGPのConnect状態では、ルーターは最初のTCP SYNを送信していますが、ピアからSYN/ACKを受信していないため、TCPハンドシェイクが完了せず、隣接関係を確立できません。

質問: **15**

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. FIN ACKを待機中のTCPセッション

B. SYN ACKを待機しているTCPセッション

C. パケットの送受信を伴うUOPセッション

D. 受信パケットが1つだけのUDPセッション

正解: **B,D (**コメントを発表する**)**

質問: **16**

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。

```
# get router info routing-table database
---omitted---

Routing table for VRF=0
S           0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S           0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive, [50/0]
---omitted---
```

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？

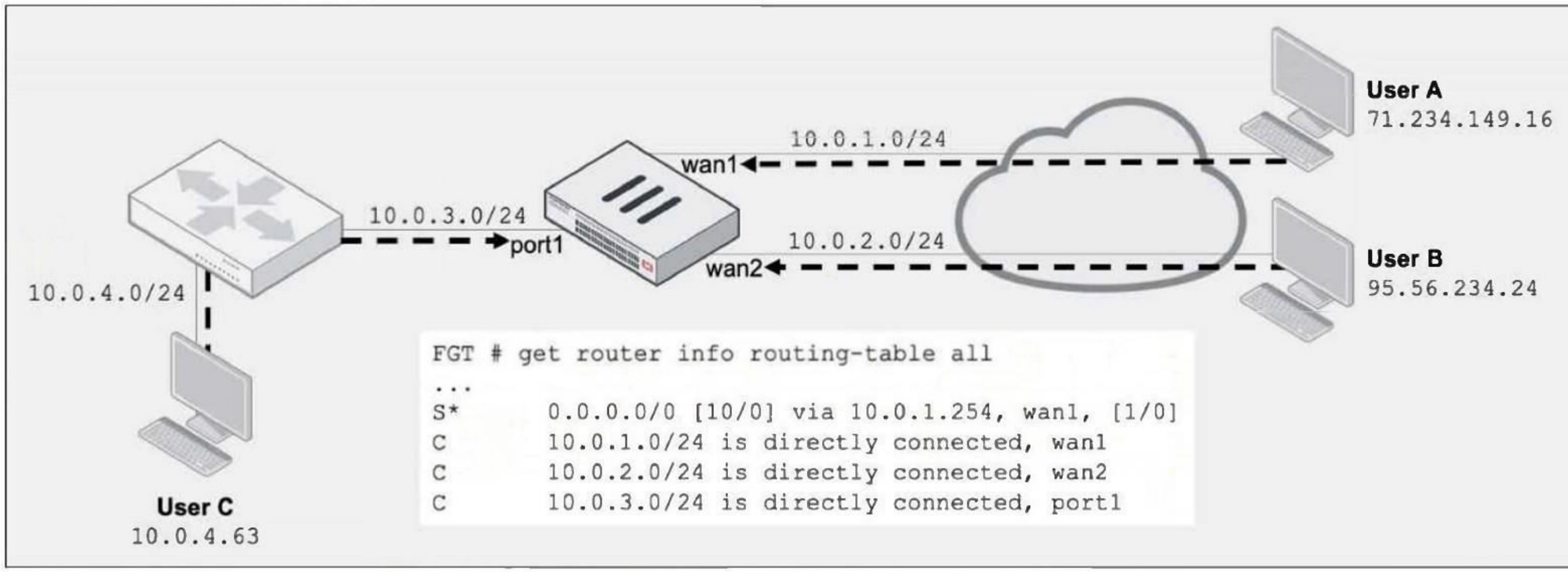
A. 出力に表示されている2つのデフォルトの静的ルートは両方ともFIBに注入されます。
B. port2 のデフォルト静的ルートが転送情報ベース (FIB) に挿入されます。
C. port1 のデフォルト静的ルートが FIB に注入されます。
D. 出力に示されているどちらの経路もFIBには注入されません。
正解: **B** (コメントを発表する)

質問: **17**
デバッグコマンドの出力例を含む図を参照してください。

```
# diagnose hardware sysinfo conserve
memory conserve mode:                    on
total RAM:                               3040 MB
memory used:                             2706 MB 89% of total RAM
Memory freeable:                          334 MB 11% of total RAM
memory used + freeable threshold extreme:  2887 MB 95% of total RAM
memory used threshold red:               2675 MB 88% of total RAM
memory used threshold green:             2492 MB 82% of total RAM
```

デフォルト設定が適用されている場合、展示図に示されている節約モードについて、どのような結論を導き出せますか？
A. FortiGateは現在、フローベースのコンテンツ検査を必要とする新規セッションを許可し、プロキシベースのコンテンツ検査を必要とするセッションをブロックしています。
B. FortiGateは現在、フローベースまたはプロキシベースのコンテンツ検査を必要とする新しいセッションを許可していますが、それらのセッションに対して検査は実行していません。
C. FortiGate は現在、メモリ使用量が多いため、コンテンツ検査の要件や構成設定に関係なく、すべての新しいセッションをブロックしています。
D. FortiGateは現在、フローベースまたはプロキシベースのコンテンツ検査を必要とする新しいセッションを許可しており、それらのセッションに対して検査を実行しています。
正解: (正解を表示します)
メモリ使用量が赤色のしきい値を超えても、極端のしきい値を下回っている場合、FortiGateの節約モードはフローベースの検査を使用する新しいセッションを許可しますが、プロキシベースの検査を必要とするセッションは拒否します。

質問: **18**
図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。）




```
FGT # get router info routing-table all
...
S*      0.0.0.0/0 [10/0] via 10.0.1.254, wan1, [1/0]
C       10.0.1.0/24 is directly connected, wan1
C       10.0.2.0/24 is directly connected, wan2
C       10.0.3.0/24 is directly connected, port1
```

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: パス。FortiGateはwan1を使用して非対称ルーティングを使用してトラフィックに応答します。
95.56.234.24。
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**)**
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。
95.56.234.24 は 10.0.2.0/24 と一致しないため、wan2 に到着したトラフィックは wan1 のデフォルト ゲートウェイを経由してルーティングされる必要があり、厳密な逆パス チェックによって破棄されます。
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。
Port1は10.0.3.0/24についてしか認識していません。10.0.4.0/24に対する静的ルートまたはプロキシARPがない場合、FortiGateはそのトラフィックを受け入れたりルーティングしたりしません。
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。
71.234.149.16 からのトラフィックは wan1 に到達し、戻り経路も wan1 (デフォルトルート) を経由するため、成功します。

質問: **19**
添付資料には、フェーズ1の設定画面のスクリーンショットが含まれています。VPNは起動していません。

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. 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。
B. diagnose debug application ike -1 を diagnose debug application ipsec -1 に置き換えます。
C. 管理者は、diagnose debug enable コマンドも実行する必要があります。
D. 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。
正解: **(**正解を表示します**)**

質問: **20**
図を参照してください。この図は、SAML接続を診断するためにコマンド「diagnose debug application samld -1」を使用した際の出力結果を示しています。

```
**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC718A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><sa
ml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:
NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProvide
rID>http://10.1.10.2/saml-idp/nst/metadata/</lasso:RemoteProviderID><lasso:Msg
Url>https://10.1.10.2/saml-
idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL30W5sAZtBwhhEEtQF0AdfTN0u0GRrZ2%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhbw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7IVha7IGXKZEIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>
```

この出力結果に基づいて、どのような結論が得られますか？

A. 認証にはActive Directoryが使用されます。

B. 認証要求はSSL VPN接続用です。

C. IdP IP アドレスは 10.1.10.254 です。

D. IdPのIPアドレスは10.1.10.2です。

正解**: D (**コメントを発表する**)**

SAML AuthnRequest の Destination URL と RemoteProviderID URL はどちらも https://10.1.10.2 を指しており、これは IdP の IP アドレスが 10.1.10.2 であることを示しています。

質問**: 21**

添付の図を参照してください。この図には、リアルタイムLDAPデバッグの出力の一部が示されています。

```
# fnbamd_fsm.c[1274] handle_req-Rcvd auth req 6750221 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=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 6750221
fnbamd_ldap.c[275] get_all_dn-Found no DN
fnbamd_ldap.c[298] start_next_dn_bind-No more DN left
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending result 1 for req 6750221
```

この問題を解決するために、管理者はどのような2つの対策を講じることができますか？ 2つ選択してください。）

A. ユーザーが 「jsmith」ではなく 「John Smith」を使用してログインするようにしてください。

B. ユーザーが正しいユーザー認証情報を提供していることを確認してください。

C. LDAP認証プロセスのステップ4が成功するように、ユーザーが少なくとも1つのADグループのメンバーであることを確認してください。

D. アカウントが有効であることを確認してください。

正解: **(**正解を表示します**)**

FortiGateのLDAP認証で一致するDNが見つからない場合、「すべてのDNを取得 - DNが見つかりませんでした」と報告されます。これは通常、ユーザーがFortiGateにチェックするように指示したグループに属していないか、アカウントが現在アクティブではないことを意味します。

ユーザーが少なくとも1つのActive Directoryグループのメンバーであることを確認してください。

FortiGateでログインを特定のグループに制限するように設定している場合、それらのグループに属していないユーザーはLDAP検索では決して見つかりません。

アカウントが有効であることを確認してください。

FortiGateのデフォルトの検索フィルターは、無効化またはロックされたアカウントを除外するため、無効化されたユーザーオブジェクトはDN検索にも表示されません。

質問: **22**

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. これは第2段階の交渉を示しています。

C. イニシエータは、IPsecピアIDとしてremoteを提供しました。

D. ローカルゲートウェイのIPアドレスは10.0.0.1です。

正解: **(**正解を表示します**)**

質問: **23**

図を参照してください。この図には、2つのルーティングデバッグコマンドの出力の一部が示されています。

ECMPを使用して、内部ユーザーからのWebトラフィックをインターネットにルーティングするには、FortiGateで管理者はどのような変更を行う必要がありますか？

A. snat-route-change を有効に設定します。

B. ポート1を使用する静的デフォルトルートの優先度を10に設定します。
C. ポート2を使用する静的デフォルトルートの優先度を1に設定します。
D. preserve-session-route を有効に設定します。
正解: **B** (コメントを発表する)

質問: **24**
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. SPログインダンプ
B. 認証応答
C. 認証要求
D. アサーションダンプ
正解: (正解を表示します)
IdPは、SAMLレスポンスの<Assertion>セクション内にユーザーのすべてのSAML属性を提供するので、それらはAssertionダンプ部分に表示されます。

質問: **25**
補助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？（2つ選択してください。）
A. 補助セッション設定が無効になっている場合、各トラフィックパスに対して、FortiGate は同じ補助セッションを使用します。
B. 補助セッション設定が有効になっている場合、ルーティング変更時に 2 つのセッションが作成されます。
C. 補助セッションの販売が無効になっているため、補助セッションのみがオフロードされます。
D. 補助セッション設定が有効になっている場合、ECMPトラフィックはNP6プロセッサに高速化されます。
正解: **B,D** (コメントを発表する)

質問: **26**
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最大しきい値に達すると、節約モードに入ります。
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、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。
C. FortiGateは、システムメモリが設定された緑色のしきい値を下回ると、節約モードを終了します。
D. 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、FortiGate はすべての新しいセッションを破棄し始めます。
正解: (正解を表示します)
メモリ使用量が緑色（低水位のしきい値を下回ると、FortiGateは自動的に省電力モードを終了します。
メモリ使用量が赤色（高水位のしきい値に達すると、FortiGateはコンテンツ検査を必要とするすべてのフローに対して、「新規セッション」のメモリ節約アクションの適用を開始します。

質問: **27**
FSSO環境では、ユーザーはFortiGate上でアクティブとして表示されますが、インターネットを閲覧することはできません。
潜在的な問題として検証する必要のない要因はどれですか？
A. コレクターエージェントとFortiGate間の接続
B. 有効なファイアウォールポリシーが存在するかどうか
C. ユーザーのグループ情報
D. ユーザーのIPアドレスがアクティブなFSSOユーザーのリストに含まれていること
正解: (正解を表示します)

質問: **28**

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. ルート FortiGate 上で下流の FortiGate を認証する必要があります。

B. FortiGateはNATモードであってはなりません。

C. 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。

D. 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。

E. 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。

正解: **(**正解を表示します**)**

ルートFortiGate上で、下流側のFortiGateを認証します。

セキュリティファブリックに参加できるのは、登録済み／承認済みのデバイスのみです。

経路上で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。

ポート8013はファブリックの制御/テレメトリセッションを伝送するため、エンドツーエンドで開いている必要があります。

上流側のFortiGateの受信インターフェースで、Security Fabric/FortiTelemetryを有効にしてください。

下流側のFortiGateとの接続を受け入れるインターフェースで、テレメトリを有効にする必要があります。

質問: **29**

図を参照してください。FortiGateでCPU使用率が継続的に高い状態を示しています。メンテナンス期間中にCLIコマンド「diagnose sys top」を実行すると、図に示すような出力が表示されます。

CLIコマンドdiagnose test application ipsmonitor 5を実行しましたが、デーモンipsenginedによるCPU使用率は低下しませんでした。

CPU使用率を効果的に削減するために、すぐにできることは何ですか？

```
# diagnose sys top
Run Time: 47 days, 11 hours and 14 minutes
      ipsengine   30049     R <     99    2.1    3
```

A. 交通量の急増がないか監視する。

B. すべてのIPSエンジンを再起動します。
C. 内部間ポリシーでIPSを無効にする。
D. アクティブなIPSプロファイルで有効になっているIPSシグネチャを確認します。
正解: **(**正解を表示します**)**
純粋に内部トラフィックに対するIPS検査を無効にすることで、ipsengineデーモンへの負荷を即座に軽減し、CPU使用率を下げることができます。シグネチャの調整やエンジンの再起動を待つ必要はありません。

質問: **30**
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[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. FortiOSはユーザーグループ情報を収集します。
B. FortiOS は LDAP 認証プロセスの第 2 段階 (検索リクエスト) を実行しています。
C. FortiOS は、ユーザーの認証情報を使用して LDAP サーバーにバインドします。
D. 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。
正解: **(**正解を表示します**)**

質問: **31**
図を参照してください。図には、コマンド diagnose vpn tunnel list の出力が含まれています。

```
# 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
```


トンネルの現状はどうなっていますか？

A. フェーズ1とフェーズ2の両方について、交渉は成功裏に終了しました。

B. フェーズ2は終了しました。

C. トンネルを車両が通過しています。

D. フェーズ1が終了しました。

正解: **(**正解を表示します**)**

重要な指標は、child_num=0 およびproxyidセクションのsa=0）であることです。これは、IPsecの子SA （フェーズ2トンネル）がアクティブではないことを意味します。フェーズ1は確立されていますが、フェーズ2のSAはネゴシエートされていません。

質問: **32**
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。この問題を解決するために、管理者はどのような2つの対策を講じるべきでしょうか？ 2つ選択してください。）
A. 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。
B. 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。
C. 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。
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**)**
両方のルーターのOSPFが有効になっているインターフェースに同じサブネットのIPアドレスが割り当てられていることを確認してください。隣接関係は同じネットワークセグメント上のピアとのみ形成されます。
IPプロトコル89（OSPF）がファイアウォールやACLによってブロックされていないことを確認してください。OSPFはTCPやUDPポートではなく、IP 89を使用します。

質問: **33**
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_Auth
C. IKE_SA_INIT
D. CREATE_CHILD_SA
正解: **D (**コメントを発表する**)**

質問: **34**
IKEv2のどのフェーズでDiffie-Helman鍵交換が行われますか？
A. IKE_SA_INIT
B. Create_CHILD_SA
C. IKE_Auth
D. IKE_Req_INIT
正解: **(**正解を表示します**)**

質問: **35**
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. 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。
D. 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。
E. 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。
正解: **(**正解を表示します**)**

質問: **36**

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。

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 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。

正解: **(**正解を表示します**)**

質問: **37**

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

コマンドの出力から何が分かりますか？

A. ローカルの FortiGate は DROther ではありません。

B. ローカルの Fortigate と OSPF ネイバー 0.0.0.10 を接続するネットワークタイプはポイントツーポイントです。

C. ローカルのFortiGateはBDRです。

D. すべての近隣はエリア 0.0.0.0 にあります。

正解: **(**正解を表示します**)**

質問: **38**

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. ユーザーはCN=John Smithを使用して認証しています。

B. 設定された LDAP サーバーの名前は Lab です。

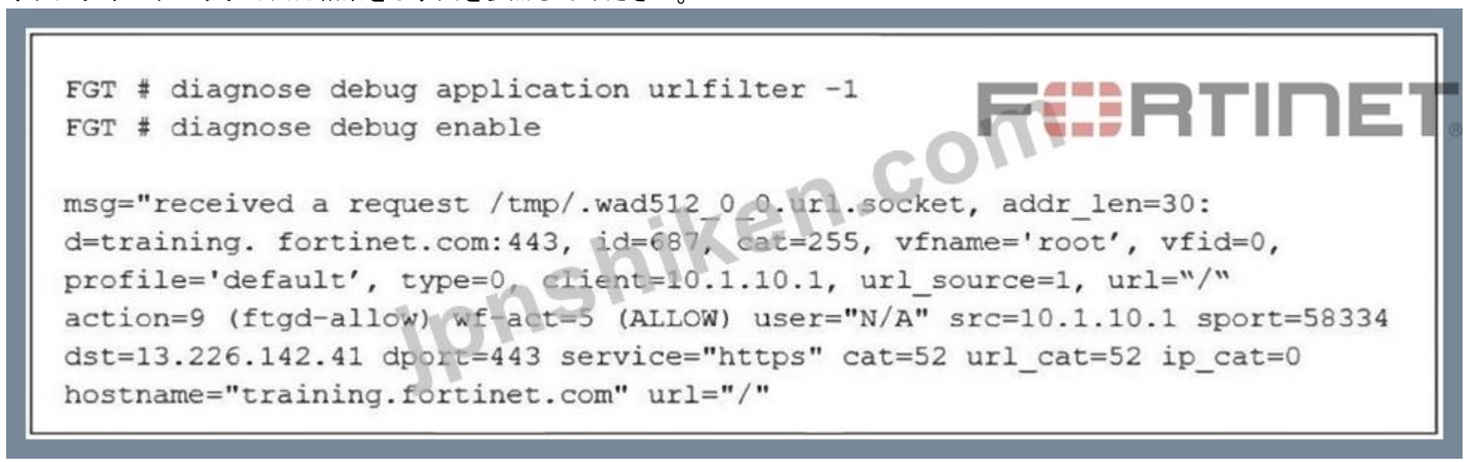
C. FortiOS は LDAP 認証プロセスの第 2 段階 (検索要求) を実行しています。

D. 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。

正解: **(**正解を表示します**)**

質問: **39**

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。



この出力結果を正確に説明しているのは、次のうちどれですか？

A. 要求されたウェブサイトへのアクセスは、ウェブフィルタプロファイル ftgd-allow によって許可されました。

B. サーバーのホスト名は、サーバー証明書の共通名 (CN)またはクライアント要求のサーバー名表示 (SNI)から抽出されました。

C. 要求されたURLはFortiGuardカテゴリID 255に属すると検出されました。

D. urlfilterdebug がカテゴリの不一致を検出しました。

正解: **(**正解を表示します**)**

hostname="training.fortinet.com"フィールドは、FortiGateがSNI (TLSクライアントHello内)を介してHTTPSホスト名を学習した場合、またはサーバー証明書のCNを解析した場合にのみ表示され、暗号化されたトンネル上のHTTPヘッダーからは取得されません。

質問: **40**

コレクターエージェントのログ出力を示す図を参照してください。

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

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は何ですか？
A. ワークステーションが休止状態から復帰しました。
B. コレクターエージェントがクラッシュしています。
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**)**
DCエージェントコレクターがワークステーションとの間でTCPポート139または445を使用してSMB/レジストリセッションを開くことができない場合、そのホストは 「未検証」とマークされます。これらのポートにアクセス可能であることを確認することで、通常はこの問題は解決します。

質問: **41**
セキュリティファブリックの通信に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. FortiTelemetryとNeighbor Discoveryはどちらもを使用して動作します。
B. 近隣探索のデフォルトポートは変更できます。
C. FortiTelemetryはFortiGateインターフェースで手動で有効にする必要があります。
D. デフォルトでは、ダウンストリームの 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。
正解: **(**正解を表示します**)**
FortiTelemetryのデフォルトのTCPポート8013は、必要に応じて変更できます。ダウンストリームのFortiGateがセキュリティファブリックに参加するには、TCPポート8013を介してアップストリームのFortiGateとのセッションを開始する必要があります。アップストリームのFortiGateがダウンストリームのFortiGateからの接続を受け入れるには、ネットワークインターフェイス（GUIの 「管理アクセス」）でセキュリティファブリック接続設定を有効にする必要があります。

質問: **42**
BGPデータベースの出力結果を示す図を参照してください。

```
# get router info bgp network
VRF 0 BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete


   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
* i0.0.0.0/0        100.64.2.254   0               100      0         0 ? <-/->
*>                  100.64.2.1                          32768         0 ? <-/1>
*> 4.2.2.1/32       100.64.2.1                          32768         0 ? <-/1>
*>i8.8.8.8/32       100.64.2.254   0               100      0         0 ? <-/1>
*>i10.20.30.0/24    172.16.54.115  0               100      0         0 i <-/1>


Total number of prefixes 4
```


正しい記述はどれですか？ 2つ選択してください。）

A. ネットワークコマンドを使用して、10.20.30.0'24 のアドバタイズされたプレフィックスが設定されました。

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

C. 10.20.30.0'24 のアドバタイズされたプレフィックスは、別のルーティングプロトコルの再配布によってアドバタイズされています。

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

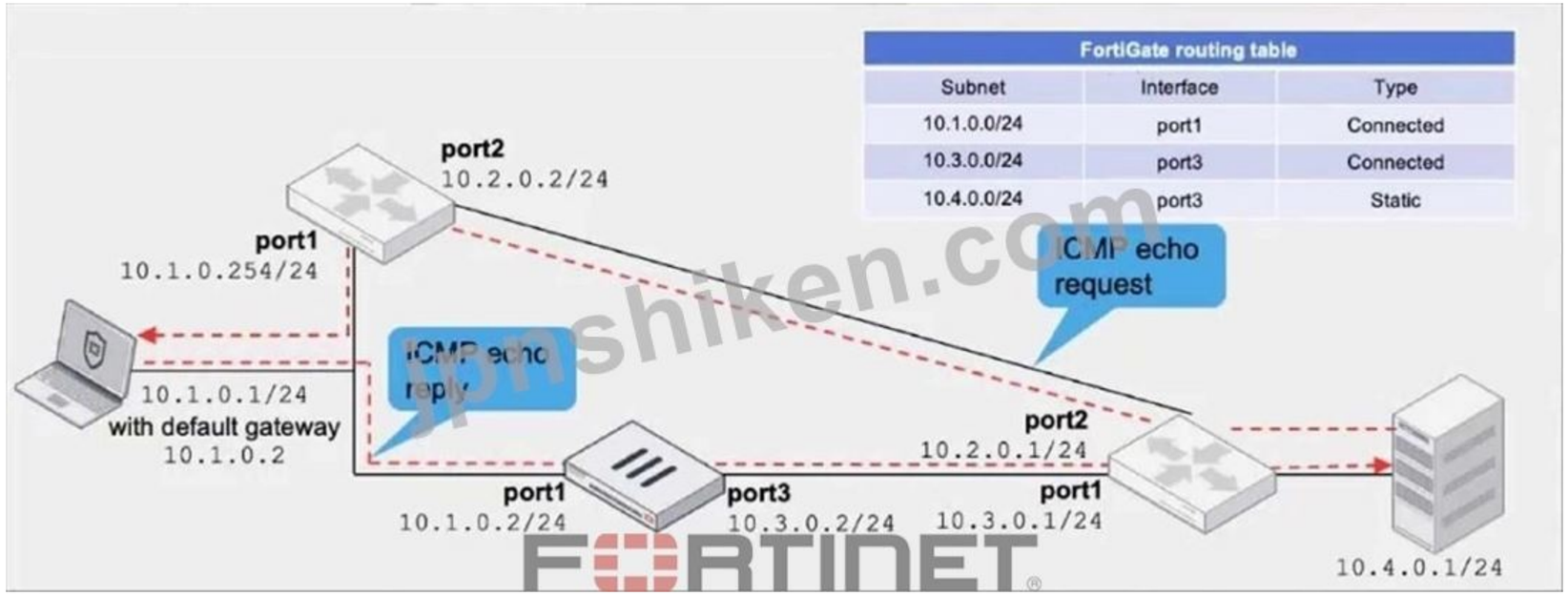
正解: **(**正解を表示します**)**

get router info bgp network は、BGP ルーティング テーブルを一覧表示します。これは、ネイバーから学習した有効な (*) および最適な (>) プレフィックスと、ローカルで生成されたプレフィックスです。

10.20.30.0/24 のエントリには発信元コード i (IGP) が表示されており、これは再配布ではなくネットワークコマンドによって注入されたことを示しています。

質問: **43**

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. 設定システム設定で非対称ルーティングを有効にします。
B. 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. 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。
D. 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。
正解: (正解を表示します)
FortiGuardはステートフルファイアウォールであるため、セッションがポート1から開始された場合でも、ICMP応答の返信を許可する明示的なポリシーが必要です。ポート3からポート1へのICMP応答を許可するファイアウォールポリシーを追加することで、ポート3に到着したエコー応答はポート1に接続されたラップトップに転送されます。この逆方向のポリシーがない場合、サーバーからの応答はFortiGateで破棄されます。これにより、10.1.0.1と10.4.0.1間の双方向ICMPフローが確保されます。

質問: **44**
図を参照してください。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して、トンネルが切断される原因として考えられることは何ですか？

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
61BBA3725BD738D3265A0B7A271799B7081005019E253B8B0000006CE306FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF6BF6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB0000002000000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B8204D890A367DBDDDB20E5812CB470F87CB15504E
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 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E38196550041FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD0000002000000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B0000002000000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000001
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 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A833800000020000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDDB812D02AE1672BD0E893431344D7BC31E9323A2C56E27DB43B747870885D7954558993B25BC43118695BEA47
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
```

A. フェーズ2は下がったが、フェーズ1は上がった。
B. デッドピア検出が確認パケットを受信していません。
C. 再鍵交換交渉中にトンネルが切断されます。
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**)**
対応する DPD 応答がないまま「notify msg received: RU-THERE」が継続的に送信されると、FortiGate はデッドピア検出タイマーが期限切れになったときに IPsec SA を削除し、トンネルをダウンさせます。

質問: **45**
図を参照してください。図には、コマンド diagnose debug rating の出力の一部が示されています。

```
-=- Server List (Mon May  6 03:47:52 2024) -=-
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  6 03:47:43 2024
64.26.151.35                              10     46           -5                329072          0       6806 Mon May  6 03:47:43 2024
66.117.56.37                              10     75           -5                 71638          0        275 Mon May  6 03:47:43 2024
65.210.95.240                             20     71           -8                 36875          0         92 Mon May  6 03:47:43 2024
209.22.147.36                             20    103 DI        -8                 34784          0       1070 Mon May  6 03:47:43 2024
208.91.112.194                            20    107 D         -8                 35170          0       1533 Mon May  6 03:47:43 2024
96.45.33.65                               60    144            0                 33728          0        120 Mon May  6 03:47:43 2024
80.85.69.41                               71    226            1                 33797          0        192 Mon May  6 03:47:43 2024
62.209.40.74                             150     97            9                 33754          0        145 Mon May  6 03:47:43 2024
121.111.236.179                           45     44  F         -5                 26410      26226      26227 Mon May  6 03:47:43 2024
```

この展示において、FortiGateのアルゴリズムはどのFDSサーバーを選択するでしょうか？

A. 66.117.56.37

B. 208.91.112.194

C. 209.22.147.36

D. 64.26.151.37

正解: **(**正解を表示します**)**

FortiGateは、64.26.151.37を選択します。これは、重みが最も低く（10）、重み10のすべてのサーバーの中で最もRTT（45ms）が低いためです。

質問: **46**

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。

D. 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。

正解: **(**正解を表示します**)**

質問: **47**

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。

```
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
```

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: **C,D** (コメントを発表する)

セッションはオフロードされました。

offload=8/8、ips_offload=1/1、in_npu=1/1 out_npu=1/1のフラグは、転送機能とIPS機能の両方がハードウェアで処理されていることを示しています。

トラフィックはポリシーID 1に一致します。

policy_id=1フィールドは、このセッションがファイアウォールポリシー1によって作成されたことを示します。

質問: 48

添付資料には、FortiGate上の2つのVPNの部分的な設定が含まれていますので、ご参照ください。

Exhibit 1

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

Exhibit 2

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


管理者は、2 つの異なるユーザー グループ用に 2 つの VPN を設定しました。Users-2 グループに属するユーザーは VPN に接続できません。診断コマンドを実行した後、管理者は FortiGate が Users-2 VPN を Users-2 グループのメンバーに対して一致させていないことを発見しました。
2グループ。問題を解決するために、管理者はどの2つの変更を行う必要がありますか？ 2つ選択してください。）

A. 両方のVPNでアグレッシブモードに変更します。
B. 両方のVPNでXAuthを有効にする。
C. 両方のVPNで異なる事前共有キーを使用します。
D. 両方のVPNで特定のピアIDを設定します。
正解: **(**正解を表示します**)**
FortiGateがIDに基づいて動的ピアを照合できるように、両方のトンネルをアグレッシブモードに変更してください。
各フェーズ1インターフェースに固有のピアIDを設定することで、ユーザー1とユーザー2に対して適切なVPNが選択されるようにします。

質問: **49**
図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。）

```
# diagnose sys top
Run Time:  0 days, 0 hours and 18 minutes
0U, 0N, 1S, 95I, 0WA, 0HI, 0SI, 0ST; 16063, 12523F
         pyfcgid      248      S       2.9      3.8  9
          newcli      251      R       0.1      1.0  5
  merged_daemons      185      S       0.1      0.7  6
         miglogd      177      S       0.0      6.8  0
         pyfcgid      249      S       0.0      3.0  2
         pyfcgid      246      S       0.0      2.8  5
         reportd      197      S       0.0      2.7  2
         cmdbsvr      113      S       0.0      2.4  7
```


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. 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。
正解: **(**正解を表示します**)**
最後の列にはCPUコアIDが表示されているので、miglogdがコア0で実行されていることがわかります。
「実行時間」の行は、システム（つまり、top コマンド）が稼働してからどれくらいの時間が経過したかを示します。
この場合は18分です。
MEM%列は、cmdbsvrがメモリの2.4%を使用していることを示しています。

質問: **50**
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: **A,D (**コメントを発表する**)**

質問: **51**

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 output

```
# 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. 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。

B. 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。

C. 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。

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**)**

このセッションのトラフィックは、フェイルオーバー後も新しいプライマリで中断されることなく継続されます。これは、セッションが既にセカンダリと同期済み（ha_id=0で「synced」状態）であるため、クライアントが接続を再確立する必要がないためです。

質問: **52**

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. FGT-8 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で構成されています。
B. 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。
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 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。
正解: (正解を表示します)

質問: **53**
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. これは10.1.10.1から10.200.5.1へのICMPセッションです。
C. 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。
D. これは 10.1.10.10 から 10.200.1.1 への ICMP セッションです。
正解: (正解を表示します)

質問: **54**

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. 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。

B. 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。

C. FortiGateはNATモードであってはなりません。

D. 下流の FortiGate をルート FortiGate で認証する必要があります。

E. 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。

正解: **(**正解を表示します**)**

質問: **55**

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. 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。

C. 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。

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: **A (**コメントを発表する**)**

質問: **56**
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=2024-02-23 09:42:29
```

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)
出力にある「Internet service(1): Fortinet-FortiGuard(...)」オブジェクトへの参照から、このポリシー ルート エントリは、従来のアドレス オブジェクトではなく、インターネット サービス データベース (ISDB) オブジェクトを使用していることが明らかです。

質問: **57**
展示資料を参照してください。

```
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
61BBA3725BD738D3265A0B7A271799B7081005019E253B8B0000006CE306FFBD5AD97F5AD027B12CAE19C5EFA091289F6D184E10DF2548B9B1FF6BF6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB0000002000000000101108D2861BBA3725BD738D3265A0B7A271799B7000014D85DB9684B6CFE9C601AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000001011080293CDB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B820AD090A367DBDDDB20E5812CB470F87CB15504E
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 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E3819655CC61FDAAF2034B0253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD0000002000000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B0000002000000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A09198EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
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 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A833800000020000000001011080293CDB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDDB812D02AE1672BD0E893431344D7BC31E9323A2C56E27DB43B747870885D7954558993B25BC43118695BEA47
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(18)2) 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. フェーズ2は低下したが、フェーズ1は上昇した。
B. 再鍵交換交渉中にトンネルが切断されます。
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. タイマーが切れるとトンネルが落下します。
正解: **C** (コメントを発表する)

質問: **58**
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。

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, VRF 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1

  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2

  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5

    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 sent 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

ローカルルーターがDR（指定ルーター）に選出されるには、何が必要ですか？

A. ローカルルーターは、再選が行われ、かつそのルーターIDが最も高い場合にのみDRに選出されます（優先順位が等しいと仮定）。

B. 現在のDRが失敗した場合、ローカルルーターはBDRよりも高いルーターIDを持っているため、DRに選出されます。

C. ローカルルーターはDRに選出されません。

D. ローカルルーターがDRに選出されるには、DRとBDRの両方が失敗する必要があります。

正解: **D** (コメントを発表する)

ブロードキャストネットワークでは、DRがダウンした場合、BDRが自動的に引き継ぎます。BDRが存在しない場合（またはBDRもダウンした場合）にのみ、新たな完全なDR選出が行われ、その時点で、残りのルーターの中で最も高いルーターIDを持つこのルーターが選ばれます。

質問: **59**

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。

```
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
```

正しい記述はどれですか？ 2つ選択してください。）

A. NP7 がこのセッションのオフロードを処理しています。

B. トラフィックは VLAN 0000 用にタグ付けされています。

C. トラフィックはポリシーID 1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**)**

質問: **60**
FortiOSの 「ユーザー半径の設定」で設定できない認証オプションはどれですか？
A. イープ
B. パパ
C. mschap2
D. mschap
正解: **(**正解を表示します**)**

質問: **61**
図を参照してください。これはFortiGateの設定例です。管理者がFortiGate上のWebフィルタの問題をトラブルシューティングしています。
管理者はWebフィルタプロファイルを設定し、それをポリシーに適用しましたが、Webフィルタはポリシーを通過するトラフィックを一切検査していません。
管理者はこの問題を解決するために何をすべきでしょうか？

FortiGate configuration

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-iD6 ::
    set proxy-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username
    set ddns-server-ip 0.0.0.0
    set dons-server-port 443
end
```

A. webfilter-force-off を無効にします。

B. VDOM レベルで webfilter-force-off を無効にします。

C. sdns-server-ipをservice.fortiguard.netに設定します。

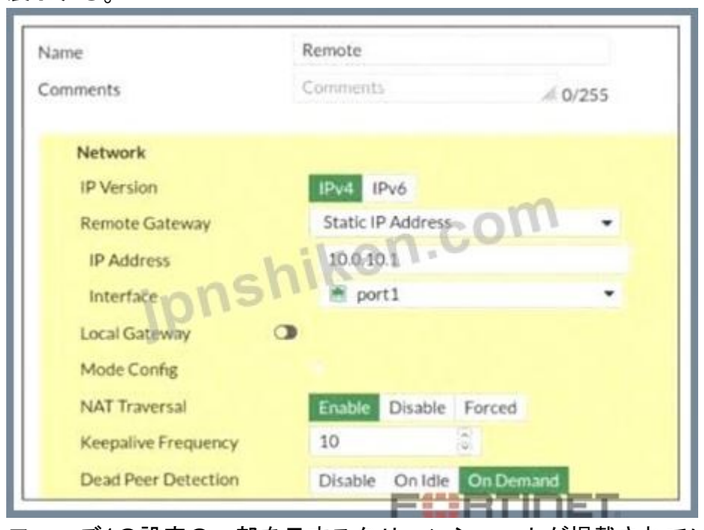
D. プロトコルをTCPに、ポートを53に変更します。

正解: (正解を表示します)

ウェブフィルタリングのグローバルな 「キルスイッチ」がオンになっています（set webfilter-force-off enable）。これにより、すべてのウェブフィルタがバイパスされます。ウェブフィルタプロファイルが実際にトラフィックを検査するようにするには、このキルスイッチをオフにする必要があります（たとえば、config system fortiguard set webfilter-force-off disableを使用します）。

質問: **62**
FortiGuardの接続問題を調査する際、どの操作が有効なトラブルシューティング手順ですか？
A. 管理用VDOMのインターネットアクセスを確認します。
B. FortiGuardのリアルタイムデバッグコマンドを使用して、評価要求を確認します。
C. 自動更新トンネリングが有効になっている場合は、DNS リクエストがプロキシされていることを確認します。
D. 仮想IPを設定して、ポート443をFortiGateの外部IPに転送します。
正解: (正解を表示します)

質問: **63**
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. diagnose debug application ike -1 を diagnose debug application ipsec -1 に置き換えます。
D. 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。
正解: (正解を表示します)