Fortinet.NSE7_EFW-6.4.v2022-01-22.q68

試験コード：	NSE7_EFW-6.4
試験名称：	Fortinet NSE 7 - Enterprise Firewall 6.4
認証ベンダー：	Fortinet
無料問題の数：	68
バージョン：	v2022-01-22
ページの閲覧量：	732
問題集の閲覧量：	11913

https://www.jpnshiken.com/shiken/Fortinet.NSE7_EFW-6.4.v2022-01-22.q68.html

質問: **1**
管理者は、HAクラスタ用に2つのFortiGateデバイスを設定しました。管理者は、HAフェイルオーバーのテスト中に、ネットワーク内の一部のスイッチが以前のプライマリデバイスにトラフィックを送信し続けていることに気付きました。管理者は、link-failed-signalの設定を有効にして、問題を修正することにしました。
この設定について正しい説明はどれですか。
A. フェイルオーバーが発生している間、以前のプライマリデバイスにハートビート以外のすべてのインターフェイスを1秒間強制的にシャットダウンします。
B. 接続されているすべてのデバイスにARPパケットを送信し、フェイルオーバー後に新しいマスターを介してHA仮想MACアドレスに到達できることを示します。
C. フェイルオーバー後2秒間、すべてのHAメンバーのすべての非ハートビートインターフェイスを無効にしました。
D. 接続されているすべてのデバイスにリンク失敗信号を送信します。
正解: **A** (コメントを発表する)

質問: **2**
いくつかのフェーズ1設定のスクリーンショットが含まれている展示を表示してから、以下の質問に答えてください。



VPNが稼働しており、DPDパケットが両方のIPsecゲートウェイ間で交換されています。ただし、トラフィックはトンネルを通過できません。診断するには、管理者は次のCLIコマンドを入力します。

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

ただし、IKEリアルタイムデバッグでは出力は表示されません。どうして？

A. デバッグ出力には、フェーズ1とフェーズ2のネゴシエーションのみが表示されます。トンネルが起動すると、それ以上の出力は表示されません。

B. デバッグ出力はフェーズ1ネゴシエーションのみを示します。その後、管理者は次のリアルタイムデバッグを有効にする必要があります。diagnosedebugapplication ipsec-1。

C. ログフィルターの設定が正しく設定されていません。VPNのトラフィックがこのフィルターと一致しません。

D. デバッグはエラーメッセージのみを表示します。出力がない場合、トンネルは正常に動作しています。

正解: **(**正解を表示します**)**

質問: **3**

次のイベントのうち、HAクラスター内の新しいプライマリユニットの選出をトリガーできるのはどれですか？ 2つ選択してください。）

A. プライマリユニットの監視対象インターフェイスの1つが切断されています。

B. プライマリユニットがHAハートビートの送信を停止します

jpnshiken.com

C. セカンダリユニットがHAクラスターから削除されます。
D. プライマリユニットのFortiGuardライセンスが更新されます。
正解: **A,B (**コメントを発表する**)**

質問: **4**
IKEリアルタイムデバッグの部分的な出力を含む展示を表示してから、以下の質問に答えてください。

```
ike 0: comes 10.0.0.2:500-> 10.0.0.1:500, ifindex-7....
ike 0: IKEV1 exchange-Aggressive id-baf47d0988e9237f/2f405ef3952f6fda len 430
ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA01100400000000000000001AE0400003C000000010000000100000030010100
ike 0: RemoteSite:4: initiator: aggressive mode get 1st response
ike 0: RemoteSite:4: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0: RemoteSite:4: VID DPD AFCAD71368A1F1c96B8696FC77570100
ike 0: RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0: RemoteSite:4: peer is FortiGate/FortiOS (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
ike 0: RemoteSite:4: negotiation result
ike 0: RemoteSite:4: proposal id = 1:
ike 0: RemoteSite:4:    protocol id = ISAKMP:
ike 0: RemoteSite:4:         trans_id = KEY_IKE.
ike 0: RemoteSite:4:         encapsulation = IKE/none
ike 0: RemoteSite:4:              type=OAKLEY_ENCRYPT_ALG,  val=AES_CBC, key-len=128
ike 0: RemoteSite:4:              type=OAKLEY_HASH_ALG, val=SHA
ike 0: RemoteSite:4:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: RemoteSite:4:              type=OAKLEY_GROUP, val=MODP1024.
ike 0: RemoteSite:4: ISAKMP SA lifetime=86400
ike 0: RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key
16:B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0: RemoteSite:4: PSK authentication succeeded
ike 0: RemoteSite:4: authentication OK
ike 0: RemoteSite:4: add INITIAL-CONTACT
ike 0: RemoteSite:4: enc
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000000801400001 81F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_12send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

このデバッグ出力に関する正しい説明はどれですか？ 2つ選択してください。）
A. ネゴシエーションはCBCハッシュでAES128暗号化を使用しています。
B. イニシエーターがIPsecピアIDとしてリモートを提供しました。
C. リモートゲートウェイのIPアドレスは10.0.0.1です。
D. フェーズ1のネゴシエーションを示しています。
正解: **(**正解を表示します**)**

質問: **5**
管理者は、FortiGateのメモリ使用量を最適化するために、すべてのTCPセッションタイマーを減らしました。ただし、変更後、1つのネットワークアプリケーションで問題が発生し始めました。トラブルシューティング中に、管理者は、クライアントがSYNパケットを送信した後、SYN / ACKが到着する前に、FortiGateがセッションを削除することに気づきました。SYN / ACKパケットがFortiGateに到着したとき、ユ

ニットはすでにそれぞれのセッションを削除しています。この問題を解決するには、どのTCPセッションタイマーを増やす必要がありますか？

A. TCPが半分開いています。

B. TCPが半分閉じています。

C. TCP時間待機。

D. TCPセッションの存続時間。

正解: **(**正解を表示します**)**

説明

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhe lp.htm？context = fgt＆file = CLI_get_Commands.58.25.html tcp-halfopen-timerは、SYNパケット、SYN / ACKのないセッションがテーブルに残ります。

tcp-halfclose-timerは、FINパケットの後、FIN / ACKのないセッションがテーブルに残る時間を制御します。

tcp-timewait-timerは、FIN / ACKパケットの後、セッションがテーブルにとどまる時間を制御します。閉じられたセッションは、シーケンス外のパケットを許可するために、さらに数秒間セッションテーブルに残ります。

質問: **6**

部分的なルーティングテーブルを含む展示を表示してから、以下の質問に答えてください。



適切なファイアウォールポリシーがすべて設定されているとすると、FortiGateは次のどのpingをルーティングしますか？ 2つ選択してください）。

A. 送信元IPアドレス10.72.3.27、宛先IPアドレス10.1.0.52。

B. 送信元IPアドレス10.1.0.24、宛先IPアドレス10.72.3.20。

C. 送信元IPアドレス10.72.3.52、宛先IPアドレス10.1.0.254。

D. 送信元IPアドレス10.73.9.10、宛先IPアドレス10.72.3.15。

正解: **A,C (**コメントを発表する**)**

質問: **7**

内部セグメンテーションファイアウォール（ISFW）の目的は何ですか？

A. 企業のDMZ内のサービスを保護するために、着信トラフィックを検査します。

B. これはネットワーク境界での最初の防衛線です。

C. 侵害の影響を最小限に抑えるために、ネットワークを複数のセキュリティセグメントに分割します。

D. 企業ネットワークを拡張するためにリモートサイトに配置されるオールインワンのセキュリティアプライアンスです。

正解: **C (**コメントを発表する**)**

説明

ISFWは、ネットワークを複数のセキュリティセグメントに分割します。それらは、内部からの攻撃からの侵害コンテナとして機能します。

質問: **8**

診断sysセッションリストの出力が含まれている展示を参照してください。



プライマリユニットのHAIDがゼロ (0)の場合、出力に関するどのステートメントが正しいですか？

A. このセッションの検査はスレーブユニットにオフロードされました。

B. マスターユニットがこのトラフィックを処理しています。

C. このセッションはスレーブユニットと同期できません。

D. このセッションはHAハートビートトラフィック用です。

正解: **B** (コメントを発表する)

質問: **9**

BGPデバッグコマンドの出力が含まれている展示を参照してください。



展示について正しい説明はどれですか？

A. カウンターが最後にリセットされてから、10.200.3.1ピアがダウンしたことはありません。

B. ローカルルーターが100.64.3.1とのTCPセッションを確立していません。

C. ローカルルーターのBGP状態は、10.127.0.75ピアのOpenConfirmです。

D. ローカルルーターは、すべてのピアから合計3つのBGP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: **10**

デバッグコマンドの出力を含む展示を表示してから、以下の質問に答えてください。

```
# 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, 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 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

jpshiken.com

展示物に関する次の説明のうち、正しいものはどれですか。2つ選択してください。）

A. ローカルFortiGateがOSPFバックアップ指定ルーターとして選出されました。

B. ローカルFortiGateのOSPFルーターIDは0.0.0.4です

C. ポート4のネットワークで、2台のOSPFルーターがダウンしています。

D. ポート4はOSPFバックボーンエリアに接続されています。

正解: **(**正解を表示します**)**

質問: **11**

2つの独立したFortiGateHAクラスタが同じブロードキャストドメインに接続されています。管理者は、両方のクラスターが同じHA仮想MACアドレスを使用していることを報告しました。これにより、ネットワークで重複したMACアドレスの問題が発生します。問題を解決するには、HAクラスターの1つでどのHA設定を変更する必要がありますか？

A. グループID。

B. グループ名。

C. セッションピックアップ。

D. GratuitousARP。

正解: **(**正解を表示します**)**

説明

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

質問: **12**

IBGPネットワークのBGPセッションの数を減らすために使用できる構成はどれですか。

A. 隣接範囲

B. ルートリフレクター

C. ネクストホップセルフ

D. 隣人グループ

正解: **(**正解を表示します**)**

説明

ルートリフレクタは、AS内のIBGPセッションの数を減らすのに役立ちます。ルートリフレクタは、あるピアから学習したルータを他のピアに転送します。ルートリフレクタを設定する場合、フルメッシュのIBGPネットワークを作成する必要はありません。クラスタ内のすべてのクライアントは、同期ルーティングの更新を取得するためにリフレクタをルーティングするためだけにタルクします。ルートリフレクタは、AS内の他のルートリフレクタおよびボーダールータにルーティングアップデートを渡します。

質問: **13**
2つのルーティングデバッグコマンドからの次の部分的な出力を調べます。次に、以下の質問に答えてください。
#ルーター情報カーネルを取得
tab = 254 vf = 0 scope = 0type = 1 proto = 11 prio = 00.0.0.0 / 0.0.0.0 / 0-> 0.0.0.0/0 pref = 0.0.0.0 gwy = 10.200.1.254 dev = 2 (port1)tab = 254 vf = 0 scope = 0type = 1 proto = 11 prio = 10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref = 0.0.0.0 gwy = 10.200.2.254 dev = 3 (port2)tab = 254 vf = 0 scope = 253type = 1 proto = 2 prio = 0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref = 10.0.1.254 gwy = 0.0.0.0 dev = 4 (port3)
#get router info routing-table all s * 0.0.0.0 / 0 [10/0] via 10.200.1.254、portl [10/0] via 10.200.2.254、port2、
[10/0] dO.0.1.0 / 24が直接接続され、port3 dO.200.1.0 / 24が直接接続され、portl d0.200.2.0 / 24が直接接続され、port2どのアウトバウンドインターフェイスが使用されるかこのFortiGateは、内部ユーザーからインターネットにWebトラフィックをルーティングしますか？
A. ポート！
B. port1とport2の両方。
C. ポート3。
D. ポート2。
正解: **D** (コメントを発表する)

質問: **14**
管理者は、IPアドレス10.0.1.254のFortiGateユニットのGIUに接続できません。管理者は、HTTPを使用して接続を試行しながら、デバッグフローを実行します。デバッグフローの出力は、展示に示されています。



デバッグフローによって表示されるエラーに基づいて、この問題の正当な理由はどれですか？ 2つ選択してください。）
A. HTTPからHTTPSへの管理アクセスのリダイレクトが無効になっています。
B. HTTP管理アクセスは80以外のポート番号で構成されています。
C. HTTP管理アクセスは、IPアドレス10.0.1.254のFortiGateインターフェースで無効になっています。
D. リバースパス転送チェックのため、パケットは拒否されました。
正解: (正解を表示します)

質問: **15**
aFortiGateセッションでのダーティフラグとはどういう意味ですか？
A. ウイルス対策検査によってトラフィックがブロックされました。

B. 次のパケットはファイアウォールポリシーに対して再評価する必要があります。
C. HAフェイルオーバー後に、セッションを以前のプライマリユニットから削除する必要があります。
D. トラフィックは許可されていないアプリケーションからのものとして識別されました。
正解: **B** (コメントを発表する)
説明
https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1

質問: **16**
2つのシステムデバッグコマンドからの次の部分的な出力を調べます。次に、以下の質問に答えてください。

```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal 1179648 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concervemode: 0
shm last entered: n/a
system last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912
SHM FS alloc: 7110656
```

上記の出力に関して正しい説明は次のうちどれですか。(2つ選択してください。)
A. キャッシュされた値は、常にアクティブな値に非アクティブな値を加えたものです
B. カーネルはメモリページングを介して間接的に低メモリ(LowTotal)にアクセスします
C. ユニットは32ビットのFortiOSを実行しています
D. ユニットはカーネル保存モードです
正解: (正解を表示します)

有効的な**NSE7_EFW-6.4**問題集はJPNTest.com提供され、**NSE7_EFW-6.4**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE7_EFW-6.4**試験問題集を提供します。JPNTest.com NSE7_EFW-6.4試験問題集はもう更新されました。ここで**NSE7_EFW-6.4**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/NSE7_EFW-6.4-mondaishu　**124**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
FortiGateデバイスのクラッシュログにはどのようなイベントが記録されていますか？ 2つ選択してください。）
A. プロセスがクラッシュします。
B. 構成が変更されました。
C. FortiGuardライセンスのステータスの変更。
D. プロキシ保存モードに出入りするシステム。
正解: **A,D** (コメントを発表する)
デバッグクラッシュログ読み取りの診断
275 :2014-08-0513 :03 :53プロキシ=アクセプターサービス= imapセッション失敗モード=アクティブ化276 :2014-08-0513 :03 :53プロキシ=アクセプターサービス= ftpセッション失敗モード=アクティブ化277 :2014- 08-05 13:03:53 proxy = acceptor service = nntp session fail mode = activate 278 :2014-08-06 11:05:47 service = kernel conserve = on free = "45034 pages" red = "45874 pages" msg = "Kernel 279 : 2014-08-0611 :05 :47は保存モードに入ります" 280 :2014-08-06 13:07:16 service = kernel conserve = exit free = "86704ページ" green = "68811ページ" 281 :2014-08-06 13:07:16 msg = "カーネルは保存モードを終了します" 282 :2014-08-06 13:07:16 proxy = imd sysconserve = exited total = 1008 free = 349 marginenter = 201 283 :2014- 08-06 13:07:16 marginexit = 302

質問: **18**
診断コマンドの部分的な出力を含む展示を表示してから、以下の質問に答えてください。

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.2.0/255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
     ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
  ah=sha1 key20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

出力に基づいて、次のステートメントのどれが正しいですか？

A. クイックモードセレクターが無効になっています。

B. DPDが無効になっています。

C. リモートゲートウェイIPは10.200.5.1です。

D. 返信防止が有効になっています。

正解: **(**正解を表示します**)**

質問: **19**

2つのWebフィルターデバッグコマンドからの部分的な出力を調べます。次に、以下の質問に答えてください。

```
# diagnose test application urlfilter 3
Domain | IP    DB Ver   T URL
34000000| 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
   34 Finance and Banking
   37 Search Engines and Portals
   43 General Organizations
   49 Business
   50 Information and Computer Security
   51 Government and Legal Organizations
   52 Information Technology
```

ipnshiken.com

上記の出力に基づいて、WebサイトwwwのFortiGuardWebフィルタカテゴリはどれですか。

A. ビジネス。

B. 一般的な組織。

C. 情報技術。

D. 金融と銀行

正解: **A** (コメントを発表する)

質問: **20**

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、どの2つの状態ですか？ 2つ選択してください。）

A. パケットが送受信されるUDPセッション。

B. FINACKを待機しているTCPセッション。

C. パケットが1つだけ受信されたUDPセッション。

D. スリーウェイハンドシェイクの完了を待機しているTCPセッション。

正解: **A,B** (コメントを発表する)

質問: **21**

2つのルーティングデバッグコマンドからのこれらの部分的な出力を表示します。

```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254
dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                  [10/0] via 10.200.2.254, port2, [10/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
```

FortiGateは、内部ユーザーからインターネットにWebトラフィックをルーティングするためにどのアウトバウンドインターフェイスを使用しますか？

A. ポート1

B. ポート1とポート2の両方

C. ポート2

D. ポート3

正解: **A (**コメントを発表する**)**

質問: **22**

管理者は、FortiGateのメモリ使用量を最適化するために、すべてのTCPセッションタイマーを減らしました。ただし、変更後、1つのネットワークアプリケーションで問題が発生し始めました。トラブルシューティング中に、管理者は、クライアントがSYNパケットを送信した後、SYN / ACKが到着する前に、FortiGateがセッションを削除することに気づきました。SYN / ACKパケットがFortiGateに到着したとき、ユニットはすでにそれぞれのセッションを削除しています。この問題を解決するには、どのTCPセッションタイマーを増やす必要がありますか？

A. TCPが半分開いています。

B. TCPが半分閉じています。

C. TCP時間待機。

D. TCPセッションの存続時間。

正解: **A (**コメントを発表する**)**

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html tcp-halfopen-timerは、SYNパケット、SYN / ACKのないセッションがテーブルに残ります。tcp-halfclose-timerは、FINパケットの後、FIN / ACKのないセッションがテーブルに残る時間を制御します。tcp-timewait-timerは、FIN / ACKパケットの後、セッションがテーブルにとどまる時間を制御します。閉じられたセッションは、シーケンス外のパケットを許可するために、さらに数秒間セッションテーブルに残ります。

質問: **23**

get sys ha statusの出力を含む展示を表示してから、以下の質問に答えてください。

```
NGFW # get sys ha status
HA Health Status: ok
Model: FortiGate0VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 01:07:35
Master selected using:
  <2017/04/24 09:43:44> FGVM010000077649 is selected as the master because it has the largest value of override pr
  <2017/04/24 08:50:53> FGVM010000077 is selected as the master because it's the only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
  FGVM010000077649(updated 1 seconds ago): in-sync
  FGVM010000077650(updated 0 seconds ago): out-of-sync
System Usage stats:
  FGVM010000077649(updated 1 seconds ago):
     sessions=30, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-60%
  FGVM010000077650(updated 0 seconds ago):
     sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-61%
HBDEV stats:
  FGVM010000077649(updated 1 seconds ago):
     port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7358367/17029/25/0, tx=7721830/17182/0/0
  FGVM010000077650(updated 0 seconds ago):
     port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7793722/17190/0/0, tx=8940374/20806/0/0
Master: NGFW         , FGVM010000077649
Slave : NGFW-2       , FGVM010000077650
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FGVM0100000077649
Slave :1 FGVM0100000077650
```

出力に関して正しいステートメントはどれですか？ (2つ選択してください。)

A. HA管理IPは169.254.0.2です。

B. ポート7は、クラスター内のすべてのデバイスでHAハートビートとして使用されます。

C. スレーブ構成がマスターと同期されていません。

D. マスターは、クラスター内の唯一のデバイスであるため、選択されています。

正解: **B,C** (コメントを発表する)

質問: **24**

展示に示されている「diagnosesyssessionlistexpectation」コマンドの出力を調べます。以下の質問に答えるよりも。

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag=·00000000·sockport=0·av_idx=0·use=3¶
origin-shaper=¶
reply-shaper=¶
per-ip_shaper=¶
ha_id=0·policy_dir=1·tunnel=/¶
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)¶
hook= pre dir=org act=noop 0.0.0.0.:0-> 0.0.0.0:0 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0·policy_id=1·auth_info=0·chk_client_info=0·vd=0
serial1=000000e9·tos=ff/ff·ips_view=0 app_list=0·app=0
dd type=0·dd_mode=0¶
```

展示会のセッションに関して正しい説明はどれですか？

A. FortiGateから発信されたトラフィック用です。

B. セッションヘルパーまたはALGによって作成されました。

C. FotiGuardからのプッシュ更新を可能にするためにFortiGateカーネルによって作成されました。

D. FortiGateで終了する管理トラフィック用です。

正解: **(**正解を表示します**)**

質問: **25**

BGPデバッグコマンドの出力が含まれているexhibitを参照してください。



10.200.3.1ピアの状態がConnectである理由を説明するステートメントはどれですか？

A. ローカルルータはリモートピアからBGPキープアライブを受信していますが、ローカルピアはまだOpenConfirmを受信していません。

B. 10.200.3.1へのTCPセッションは、3ウェイハンドシェイクを完了していません。

C. ローカルルータはピアからBGPキープアライブを受信していますが、BGPプレフィックスをまだ受信していません。

D. ローカルルーターがリモートピアからBGPプレフィックスを受信しました。

正解: **B** (コメントを発表する)
BGPネイバーの状態とその変化 :*アイドル：初期状態接続：正常な3方向TCP接続を待機中*アクティブ :TCPセッションを確立できません* OpenSent :ピアからのOPENメッセージを待機中* OpenConfirm：待機中ピアからのキープアライブメッセージ*確立済み :ピアはOPENメッセージとキープアライブメッセージを正常に交換しました

質問: **26**
デバッグコマンドの出力を示す展示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, 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 inervals 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 send 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
```

出力に関する2つの説明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. ローカルのFortiGateOSPFルーターIDは0.0.0.4です。
B. ポート4はOSPFバックボーンエリアに接続されています。
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. ローカルFortiGateはバックアップ指定ルーターです。
正解: **A,B** (コメントを発表する)
エリア0.0.0.0はバックボーンエリアです。

質問: **27**
FSSOコレクターエージェント（CA）のログには、次のエラーが表示されます。
レジストリへの接続に失敗しました :PIKA1026（192.168.12.232）
このエラーの理由は何でしょうか？
A. CAはワークステーションの名前を解決できません。
B. FortiGateはワークステーションの名前を解決できません。
C. CAはIPアドレス192.168.12.232でFortiGateに到達できません。
D. リモートレジストリサービスがワークステーション192.168.12.232で実行されていません。
正解: (正解を表示します)

質問: **28**
診断sysセッションリストの出力が含まれている展示を参照してください。

```
# 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=2171/31/1 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/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

プライマリユニットのHAIDがゼロ（0）の場合、出力に関するどのステートメントが正しいですか？

A. マスターユニットがこのトラフィックを処理しています。

B. このセッションはスレーブユニットと同期できません。

C. このセッションの検査はスレーブユニットにオフロードされました。

D. このセッションはHAハートビートトラフィック用です。

正解: **A** (コメントを発表する)

質問: **29**

SSL証明書検査方法を使用してHTTPSトラフィックを検査する場合、クライアントブラウザがサーバー名表示（SNI）拡張機能を提供しない場合、FortiGateはどのようにWeb要求をフィルタリングしますか？

A. FortiGateは、ユーザーのWebブラウザから要求されたURLを使用します。

B. FortiGateは、サーバー証明書の[件名]フィールドのCN情報を使用します。

C. FortiGateは、データを復号化するために完全なSSL検査方式に切り替えます。

D. FortiGateは、それ以上の検査を行わずにリクエストをブロックします。

正解: (正解を表示します)

質問: **30**

管理者がFortiManagerで次のCLIscriptを構成しましたが、実行後に管理対象デバイスに変更を適用できませんでした。

```
# conf rout stat
#     edit 0
#         set gateway 10.20.121.2
#         set priority 20
#         set device "wan1"
#     next
# end
```

スクリプトが管理対象デバイスに変更を加えなかったのはなぜですか？

A. ＃記号で始まるコマンドは実行されません。

B. CLIスクリプトは、ポリシーによって参照されている場合にのみオブジェクトを追加します。

C. CLIスクリプトでは不完全なコマンドは無視されます。

D. 静的ルートはTCLスクリプトを使用してのみ追加できます。

正解: **(**正解を表示します**)**
説明
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Scrコマンドラインで入力する場合の一連のFortiGateCLIコマンド。コメント行は番号記号（#）で始まります。コメント行は実行されません。

質問: **31**
get sys ha statusの出力を含む展示を表示してから、以下の質問に答えてください。

```
NGFW # get sys ha status
HA Health Status: ok
Model: FortiGate0VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 01:07:35
Master selected using:
  <2017/04/24 09:43:44> FGVM010000077649 is selected as the master because it has the largest value of override pr
  <2017/04/24 08:50:53> FGVM010000077 is selected as the master because it's the only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
  FGVM010000077649(updated 1 seconds ago): in-sync
  FGVM010000077650(updated 0 seconds ago): out-of-sync
System Usage stats:
  FGVM010000077649(updated 1 seconds ago):
     sessions=30, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-60%
  FGVM010000077650(updated 0 seconds ago):
     sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-61%
HBDEV stats:
  FGVM010000077649(updated 1 seconds ago):
     port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7358367/17029/25/0, tx=7721830/17182/0/0
  FGVM010000077650(updated 0 seconds ago):
     port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7793722/17190/0/0, tx=8940374/20806/0/0
Master: NGFW         , FGVM010000077649
Slave : NGFW-2       , FGVM010000077650
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FGVM0100000077649
Slave :1 FGVM0100000077650
```

出力に関して正しいステートメントはどれですか？（2つ選択してください。）
A. HA管理IPは169.254.0.2です。
B. スレーブ構成がマスターと同期されていません。
C. ポート7は、クラスター内のすべてのデバイスでHAハートビートとして使用されます。
D. マスターは、クラスター内の唯一のデバイスであるため、選択されています。
正解: **(**正解を表示します**)**

有効的な**NSE7_EFW-6.4**問題集はJPNTest.com提供され、**NSE7_EFW-6.4**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE7_EFW-6.4**試験問題集を提供します。JPNTest.com NSE7_EFW-6.4試験問題集はもう更新されました。ここで**NSE7_EFW-6.4**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/NSE7_EFW-6.4-mondaishu 124問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **32**
SIPセッションヘルパーとSIPアプリケーション層ゲートウェイ（ALG）に関して、正しい説明は次のうちどれですか。（3つ選択してください。）
A. SIPALGはSIPoverIPv6をサポートします。SIPヘルパーはそうではありません。
B. SIPヘルパーはSIP overTCPおよびUDPをサポートします。SIP ALGは、SIP overUDPのみをサポートします。
C. SIPALGはSIPHAフェイルオーバーをサポートします。SIPヘルパーはそうではありません。
D. SIPセッションヘルパーはカーネルで実行されます。SIP ALGは、ユーザースペースプロセスとして実行されます。
E. SIP ALGは、メディアトラフィックに対して予想されるセッションを作成できます。SIPヘルパーはそうではありません。
正解: **(**正解を表示します**)**

質問: **33**
2つのWebフィルターデバッグコマンドからの部分的な出力を調べます。次に、以下の質問に答えてください。

```
# diagnose test application urlfilter 3
Domain | IP      DB Ver    T URL
34000000| 34000000    16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
    34 Finance and Banking
    37 Search Engines and Portals
    43 General Organizations
    49 Business
    50 Information and Computer Security
    51 Government and Legal Organizations
    52 Information Technology
```

jpnshiken.com
FORTINET

上記の出力に基づいて、WebサイトwwwのFortiGuardWebフィルタカテゴリはどれですか。
A. 金融と銀行
B. 情報技術。
C. 一般的な組織。
D. ビジネス。
正解: **(**正解を表示します**)**

質問: **34**
管理者は、次のIpsecVPNをFortiGate構成に追加しました。
configvpn ipsec phasel -interface
RemoteSite」を編集する

セットタイプダイナミック
インターフェース「port1」を設定します
セットモードメイン
psksecret ENCLCVkCiK2E2PhVUzZeを設定します
次
終わり
config vpn ipsecphase2-interface
「RemoteSite」を編集する
フェーズ名「RemoteSite」を設定します
提案3des-sha256を設定します
次
終わり
ただし、フェーズ1のネゴシエーションは失敗しています。管理者は、Ipsec接続を試行しているときにIKFリアルタイムデバッグを実行しました。出力は展示に示されています。



フェーズ1でIPsecの問題を引き起こしているのは何ですか？
A. 着信IPsec接続が間違ったVPN構成と一致しています
B. フレーズ1モードをアグレッシブに変更する必要があります
C. 事前共有キーが間違っています
D. NAT-T設定が一致しません
正解: **(**正解を表示します**)**

質問: **35**
企業ネットワークでは、FSSOユーザーのみがインターネットにアクセスできます。FSSOユーザーの学生は、Windows ADネットワークに正常にログインした後、インターネットにアクセスできません。'diagnose debug authd fsso list'コマンドの出力には、学生がアクティブな

FSSOユーザーとして表示されません。他のFSSOユーザーは、問題なくインターネットにアクセスできます。管理者は何を確認する必要がありますか？ 2つ選択してください。）
A. ユーザー学生は、CAの無視ユーザーリストにリストされてはなりません。
B. ユーザー学生は、1つ以上の監視対象ユーザーグループに属している必要があります。
C. 学生ワークステーションのIPサブネットは、CAの信頼できるリストにリストされている必要があります。
D. 学生のユーザーグループの少なくとも1つは、FortiGateファイアウォールポリシーによって許可されている必要があります。
正解: **A,D (**コメントを発表する**)**
説明
https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

質問: **36**
IPS終了ログを表示して、以下の質問に答えてください。
＃テストアプリケーションの診断ipsmonitor 3
ipsengine終了ログ」
pid = 93 ¢fg）、期間= 5605322 $）、2017年4月19日水曜日09:57:26
コード= 11、理由：手動
このFortiGateのIPSのステータスはどうなっていますか？
A. IPSエンジンのメモリ消費量がモデル固有の事前定義値を超えました。
B. IPSデーモンでクラッシュが発生しました。
C. IPSエンジンと管理データベース間の通信に問題があります。
D. FortiGateの設定では、IPS関連のすべての機能が無効になっています。
正解: **(**正解を表示します**)**
コマンドdiagnosetest application ipsmonitorには、トラブルシューティングの目的に役立つ多くのオプションが含まれています。オプション3は、IPSエンジンプロセスが停止するたびに生成されるログエントリを表示します。これらのログが生成される理由はさまざまです。手動：構成により、IPSを実行する必要がなくなりました つまり、IPSに関連するすべての機能が無効になりました）。

質問: **37**
展示に示されている 「getrouterinfoospfinterface」コマンドの出力を調べます。次に、以下の質問に答えてください。

```
# 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, 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 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

上記の出力に関して正しい説明はどれですか？ 2つ選択してください。）

A. port4インターフェイスはOSPFバックボーンエリアに接続されています。
B. ローカルFortiGateがOSPFバックアップ指定ルーターとして選出されました。
C. port4ネットワークに接続されているOSPFルーターは少なくとも5つあります。
D. 2つのOSPFルーターがport4ネットワークでダウンしています。
正解: **(**正解を表示します**)**
BROADCASTネットワークには4つのネイバーがあり、そのうち1 * DR + 1 * BDRです。したがって、FGには4つのネイバーがありますが、隣接関係は2つだけで作成されます（DRとBDRを使用）。2人の隣人がDRother（ダウンしていない）。

質問: **38**
展示に示されているIKEリアルタイムデバッグからの部分的な出力を調べます。次に、以下の質問に答えてください。

```
#diagnose debug application ike -1
#diagnose debug enable
ike 0: ….: 75: responder: aggressive mode get 1st message…
…
ike 0: ….:76: incoming proposal:
ike 0: ….:76: proposal id = 0:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id = KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type= OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: my proposal, gw Remote:
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id= KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val= PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val =MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id= KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP1536.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0: ….:76: no SA proposal chosen
```

なぜトンネルが上がらなかったのですか？

A. 一方のIPsecゲートウェイはメインモードを使用しており、もう一方のIPsecゲートウェイはアグレッシブモードを使用しています。

B. リモートゲートウェイのフェーズ2構成が、ローカルゲートウェイのフェーズ2構成と一致しません。

C. リモートゲートウェイのフェーズ1構成が、ローカルゲートウェイのフェーズ1構成と一致しません。
D. リモートIPsecゲートウェイでIKEモード構成が有効になっていません。
正解: **(**正解を表示します**)**

質問: **39**
FortiGateのメモリ使用率を下げることができる構成の変更は何ですか？ 2つ選択してください。）
A. セッションの存続時間を短縮します。
B. 検査する最大ファイルサイズを減らします。
C. FortiGuardキャッシュの存続時間を増やします。
D. TCPセッションタイマーを増やします。
正解: **(**正解を表示します**)**

質問: **40**
2つのFortiGateデバイスがOSPF隣接関係を形成するには、どのような条件が必要ですか？ 3つ選択してください。）
A. IPアドレスは同じサブネットにあります。
B. ハローとデッドの間隔が一致します。
C. OSPF IPMTUが一致します。
D. OSPFピアIDが一致します。
E. OSPFコストが一致します。
正解: **A,B,C (**コメントを発表する**)**
説明
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_OSPF/OSPF_Bac

質問: **41**
管理者は、組み込みのスニファを使用して2つのFortiGate間のESP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の間にNATデバイスが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る必要がありますか。
A. スニファパケットを診断します 'udp port 500'
B. スニファパケットを診断します 'udp port 4500'
C. snifferpacket any'esp 'を診断します
D. スニファパケットを診断します 'udpポート500またはudpポート4500'
正解: **(**正解を表示します**)**
説明
NATなしでIKEトラフィックをキャプチャします :スニファパケットを診断します 'ホストとudpポート500'
---------- ESPをキャプチャします
NATなしのトラフィック :スニファパケットを 「ホストとesp」と診断します
---------- IKEをキャプチャします
およびESPwith NAT-T :diagnose sniffer packet any'host and （udp port 500 or udp port 4500）'

質問: **42**
展示に示されている 「getrouterinfobgpsummary」コマンドの出力を調べます。次に、以下の質問に答えてください。

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
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
10.200.3.1 4   65501        92       112        0     0      0     never     Connect

Total number of neighbors 1
```

リモートBGPピア10.200.3.1の状態がConnectである理由を説明できるステートメントはどれですか。

A. ローカルピアはリモートピアからBGPキープアライブを受信していますが、BGPプレフィックスをまだ受信していません。

B. 10.200.3.1へのBGP接続のTCPセッションがダウンしています。

C. ローカルピアは、リモートピアからプレフィックス付きのBGPを受信しました。

D. ローカルピアはリモートピアからBGPキープアライブを受信していますが、OpenConfirmをまだ受信していません。

正解: **(**正解を表示します**)**

説明

http://www.ciscopress.com/articles/article.asp?p=2756480

質問: **43**

スニファコマンドからの次の部分的な出力を調べます。次に、以下の質問に答えてください。

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
……
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

スニファーの最後にあるパケットドロップカウンターの意味は何ですか？

A. スニファーフィルターに一致しなかったパケットの数。

B. FortiGateによってドロップされたパケットの総数。

C. スニファーフィルターに一致し、FortiGateによってドロップされたパケットの数。

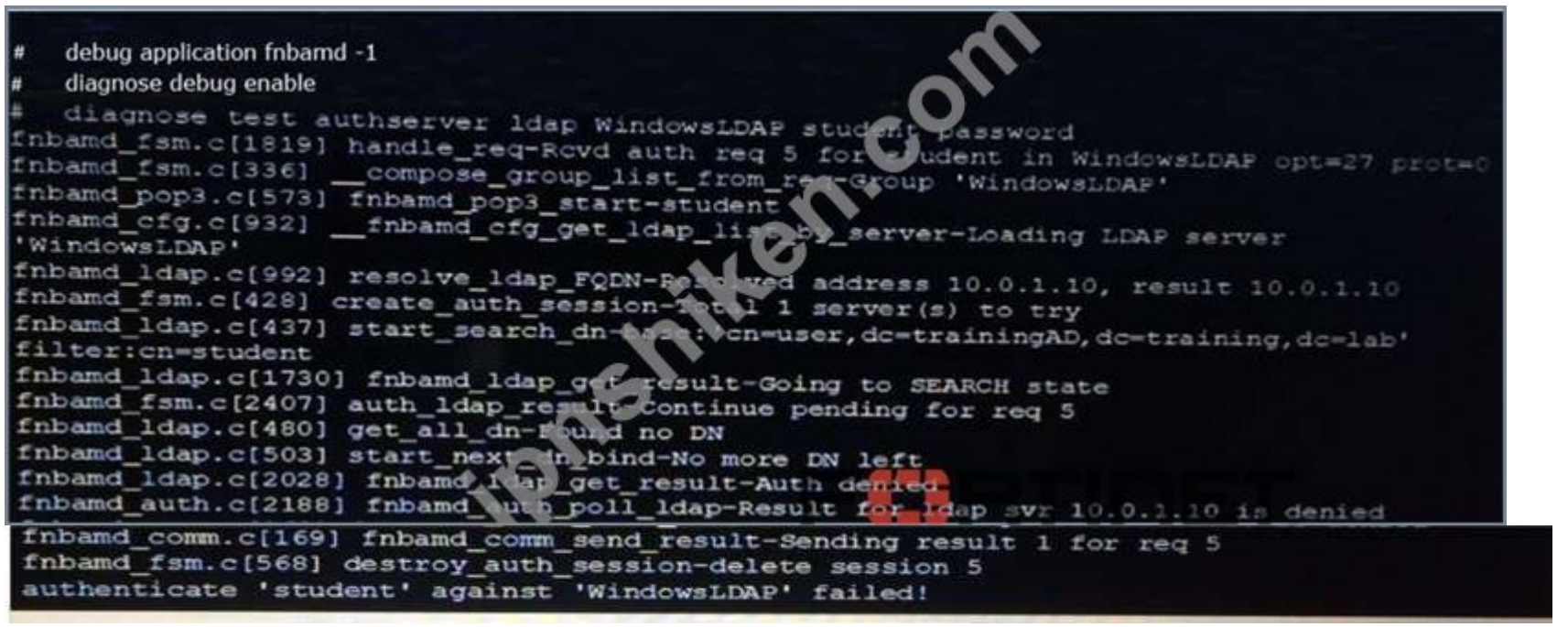
D. スニファーフィルターに一致したが、スニファーによってキャプチャできなかったパケットの数。

正解: **(**正解を表示します**)**

https://kb.fortinet.com/kb/documentLink.do?externalID=11655

質問: **44**

LDAPユーザーはFortiGateデバイスに対して認証できません。ユーザーが認証を試みたときに展示に表示されたリアルタイムのデバッグ出力を調べます。次に、以下の質問に答えてください。



展示の出力に基づいて、この認証の問題を引き起こす原因は何ですか？

A. FortiGateが間違った認証スキーマで設定されています。

B. ユーザーstudentがLDAPサーバーに見つかりません。

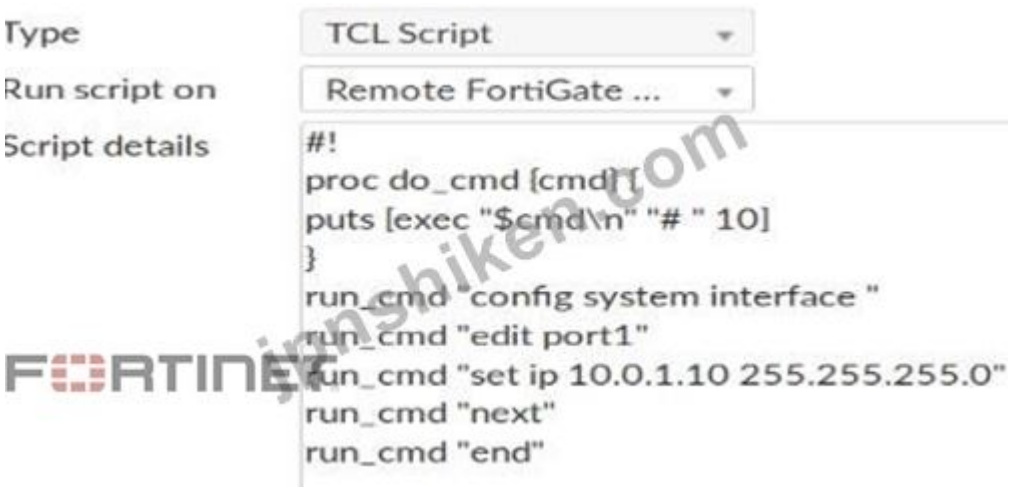
C. ユーザーの学生が間違ったパスワードを使用しています。

D. FortiGateは、LDAP管理者の間違ったパスワードで設定されています。

正解: **(**正解を表示します**)**

質問: **45**

FortiManagerのTCLスクリプト構成が含まれている展示を参照してください。



管理者がFortiManagerでTCLスクリプトを構成しましたが、実行後に管理対象デバイスに変更を適用できませんでした。

TCLスクリプトが管理対象デバイスに変更を加えられなかったのはなぜですか？

A. インターフェース構成の変更は、CLIスクリプトによってのみ実行できます。

B. TCLコマンドrun_cmdが作成されていません。

C. 不完全なコマンドはTCLスクリプトでは無視されます。

D. TCLscriptは#include <>で始まる必要があります。
正解: **(**正解を表示します**)**

質問: **46**
デバッグコマンドの出力を含む展示を表示してから、以下の質問に答えてください。



このFortiGateに関する次の説明のうち正しいものはどれですか？
A. メモリ使用量が多いため、現在プロキシ保存モードになっています。
B. メモリ使用量が多いため、現在、極端な保存モードになっています。
C. CPU使用率が高いため、現在システム保存モードになっています。
D. メモリ使用量が多いため、現在メモリ節約モードになっています。
正解: **D (**コメントを発表する**)**

有効的な**NSE7_EFW-6.4**問題集はJPNTest.com提供され、**NSE7_EFW-6.4**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE7_EFW-6.4**試験問題集を提供します。JPNTest.com NSE7_EFW-6.4試験問題集はもう更新されました。ここで**NSE7_EFW-6.4**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/NSE7_EFW-6.4-mondaishu　**124**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
管理者は、FortiGateで次のスニファを実行しています。
スニファパケットを診断する任意の「ホスト10.0.2.10」2
スニファーの出力にはどのような情報が含まれていますか？ 2つ選択してください。）
A. イーサネットヘッダー。
B. IPペイロード。
C. IPヘッダー。
D. ポート名。
正解: **(**正解を表示します**)**
https://kb.fortinet.com/kb/documentLink.do?externalID=11186

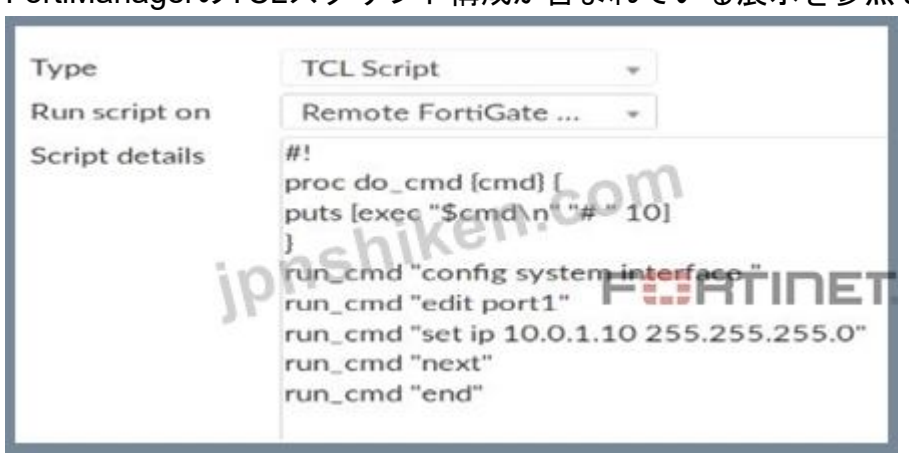
質問: **48**
CLIコマンドセットintelligent-mode <enable | disable>は、IPSエンジンの適応スキャン動作を制御します。次の文のうち、IPSアダプティブスキャンについて説明しているのはどれですか？
A. システム負荷に基づいて必要なIPSエンジンの最適数を決定します。
B. スキャン要件に基づいてFDSからオンデマンドで署名をダウンロードします。

C. セッショントラフィックのスキャンを停止するのに十分なセキュリティが確保されているかどうかを判断します。
D. 使用可能なメモリと実行されている検査のタイプに基づいてマッチングアルゴリズムを選択します。
正解: **C** (コメントを発表する)
IPSインテリジェンスの構成FortiOS5.2以降、インテリジェントモードは新しい適応型検出方法です。このコマンドはデフォルトで有効になっており、IPSエンジンがアダプティブスキャンを実行するため、一部のトラフィックでは、FortiGateがスキャンをすばやく終了し、トラフィックをNPUまたはカーネルにオフロードできます。これは、すべての既知のエクスプロイトをカバーできるバランスの取れた方法です。無効にすると、IPSエンジンはすべてのバイトをスキャンします。
config ips global set Intelligent-mode {enable | disable} end

質問: **49**
'diagnose debug authd fssolist'コマンドからの出力を調べます。次に、以下の質問に答えてください。
#diagnose debug authd fsso list -FSSO logins-IP :192.168.3.1 User :STUDENT Groups :TRAININGAD / USERS Workstation :INTERNAL2。トレーニング。LAB IPアドレス192.168.3.1は、ワークステーションINTERNAL2で使用されているものではありません。トレーニング。ラボ。
管理者は何を確認する必要がありますか？
A. ユーザーSTUDENTのログオンイベントに記録されたIPアドレス。
B. ワークステーション名INTERNAL2のDNS名前解決。トレーニング。ラボ。
C. ワークステーションINTERNAL2からFortiGateに到着するトラフィックの送信元IPアドレス。トレーニング。ラボ。
D. IPアドレス192.168.3.1の予約DNSルックアップ。
正解: **C** (コメントを発表する)

質問: **50**
FortiManagerCLIスクリプトを使用して行われた一括構成変更に関する2つの説明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. ADOMのAll FortiGateで実行すると、新しいリビジョン履歴を作成せずに変更が自動的にインストールされます。
B. デバイスデータベースで実行する場合は、インストールウィザードを使用して、管理対象のFortiGateデバイスに変更を適用する必要があります。
C. ポリシーパッケージのADOMデータベースで実行すると、変更は管理対象のFortiGateデバイスに直接適用されます。
D. リモートFortiGateで直接実行する場合、管理者はインストール前に変更を確認するオプションがありません。
正解: **B,D** (コメントを発表する)

質問: **51**
FortiManagerのTCLスクリプト構成が含まれている展示を参照してください。



管理者がFortiManagerでTCLスクリプトを構成しましたが、実行後に管理対象デバイスに変更を適用できませんでした。
TCLスクリプトが管理対象デバイスに変更を加えられなかったのはなぜですか？
A. インターフェース構成の変更は、CLIスクリプトによってのみ実行できます。
B. TCLスクリプトは#include <>で始まる必要があります。
C. 不完全なコマンドはTCLスクリプトでは無視されます。
D. TCLコマンドrun_cmdが作成されていません。
正解: **(**正解を表示します**)**

質問: **52**
管理者がRADIUS認証の問題をトラブルシューティングするために有効にする必要があるリアルタイムデバッグはどれですか？
A. デバッグアプリケーションの半径-を診断します。
B. デバッグアプリケーションfnbamd-1を診断します。
C. authd console -logenableを診断します。
D. radius console -logenableを診断します。
正解: **(**正解を表示します**)**
説明
https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838

質問: **53**
2つのルーティングデバッグコマンドからの次の部分的な出力を調べます。次に、以下の質問に答えてください。
#ルーター情報カーネルを取得
tab = 254 vf = 0 scope = 0type = 1 proto = 11 prio = 0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref = 0.0.0.0 gwy = 10.200.1.254 dev = 2 (port1)タブ= 254 vf = 0 scope = 0type = 1 proto = 11 prio = 10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref = 0.0.0.0 gwy = 10.200.2.254 dev = 3 (port2)tab = 254 vf = 0 scope = 253type = 1 proto = 2 prio = 0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref = 10.0.1.254 gwy = 0.0.0.0 dev = 4 (port3)
#get router info routing-table all s * 0.0.0.0 / 0 [10/0] via 10.200.1.254、portl [10/0] via 10.200.2.254、port2、[10/0] dO.0.1.0 / 24が直接接続されている、port3 dO.200.1.0 / 24が直接接続されている、portl d0.200.2.0 / 24が直接接続されている、port2このFortiGateが内部ユーザーからインターネットにWebトラフィックをルーティングするために使用するアウトバウンドインターフェイス？
A. port1とport2の両方。
B. ポート3。
C. ポート！
D. ポート2。
正解: **(**正解を表示します**)**

質問: **54**
BGPデバッグコマンドの出力を含む展示を表示してから、以下の質問に答えてください。

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
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
10.200.3.1   4  65501      101      115       0    0     0     never       Active

Total number of neighbors 3
```

展示品に関する次の説明のうち、正しいものはどれですか。(2つ選択してください。)

A. ピア10.125.0.60の場合、のBGP状態は確立されています。

B. BGPカウンターが最後にリセットされてから、BGPピア10.200.3.1がダウンしたことはありません。

C. ローカルBGPピアは、BGPピア10.200.3.1へのTCPセッションを確立していません。

D. ローカルBGPピアは合計3つのBGPプレフィックスを受信しました。

正解: **A,C** (コメントを発表する)

質問: **55**

AFortiGateのポートはプライベートネットワークに接続されています。そのport2はインターネットに接続されています。明示的なWebプロキシはport1で有効になっており、明示的なWebプロキシユーザーのみがインターネットにアクセスできます。Webキャッシュが有効になっていません。内部Webプロキシユーザーが HTTP経由でインターネットからファイルをダウンロードしています。このトラフィックに関連するFortiGateセッションテーブルの2つのエントリに関して正しい説明はどれですか。(2つ選択してください。)

A. セッションの1つに、送信元IPアドレスとしてport2のIPアドレスがあります。

B. 両方のセッションの宛先IPアドレスは、FortiGateのインターフェースに割り当てられたIPアドレスです。

C. 一方のセッションでプロキシフラグがオンになっていますが、もう一方のセッションではオンになっていません。

D. 両方のセッションでローカルフラグがオンになっています。

正解: **(**正解を表示します**)**

質問: **56**

FSSOコレクターエージェント(CA)のログには、次のエラーが表示されます。

レジストリへの接続に失敗しました:PIKA1026(192.168.12.232)

このエラーの理由は何でしょうか?

A. CAはワークステーションの名前を解決できません。

B. FortiGateはワークステーションの名前を解決できません。

C. リモートレジストリサービスがワークステーション192.168.12.232で実行されていません。

D. CAはIPアドレス192.168.12.232でFortiGateに到達できません。

正解: **(**正解を表示します**)**

説明
https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548

質問: **57**
FortiManagerのインストールウィザードを使用して自動化される2つのタスクはどれですか？ 2つ選択してください。）
A. 管理対象デバイスの保留中の構成変更をプレビューします。
B. FortiManagerにデバイスを追加します。
C. 管理対象デバイスからポリシーパッケージをインポートします。
D. 管理対象デバイスに構成変更をインストールします。
E. 管理対象デバイスからインターフェースマッピングをインポートします。
正解: **(**正解を表示します**)**
説明
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins 4つの主要なウィザードがあります :デバイスの追加：中央管理にデバイスを追加し、その構成をインポートするために使用されます。
インストール :デバイスマネージャーまたはポリシーとオブジェクトから管理対象デバイスへの構成変更をインストールするために使用されます。これにより、変更をプレビューでき、管理者が変更に同意しない場合は、変更をキャンセルして変更できます。
ポリシーのインポート :インターフェイスマッピング、ポリシーデータベース、および管理対象デバイスに関連付けられているオブジェクトを[ポリシーとオブジェクト]タブのポリシーパッケージにインポートするために使用されます。デフォルトではデバイスの追加ウィザードで実行され、管理対象デバイスリストからいつでも実行できます。
ポリシーの再インストール :ポリシーパッケージのクイックインストールを実行するために使用されます。管理対象デバイスにインストールされる変更をプレビューする機能はありません。

質問: **58**
FortiManagerがローカルFDSとして展開されている場合、正しい2つの説明はどれですか。 2つ選択してください。）
A. 更新サーバーまたは評価サーバーとして構成できますが、両方を構成することはできません。
B. VMライセンス検証サービスを提供します。
C. 管理対象デバイスと非管理対象デバイスの両方からの評価要求をサポートします。
D. 管理されていないデバイスで利用可能なファームウェアアップデートをキャッシュします。
正解: **(**正解を表示します**)**

質問: **59**
デバッグコマンドの出力を含む展示を表示してから、以下の質問に答えてください。



展示品に関する次の説明のうち、正しいものはどれですか。2つ選択してください。）

A. ローカルFortiGateがOSPFバックアップ指定ルーターとして選出されました。

B. ポート4のネットワークで、2つのOSPFルーターがダウンしています。

C. ローカルFortiGateのOSPFルーターIDは0.0.0.4です

D. ポート4はOSPFバックボーンエリアに接続されています。

正解: **(**正解を表示します**)**

質問: **60**

部分的なWebフィルタープロファイル構成を含む展示を表示してから、以下の質問に答えてください。

Name: default

Comments: Default web filtering. 22/255

FortiGuard category based filter

Show: Allow

- Bandwidth Consuming
  - File Sharing and Storage

Status URL Filter

Block invalid URLs

URL Filter

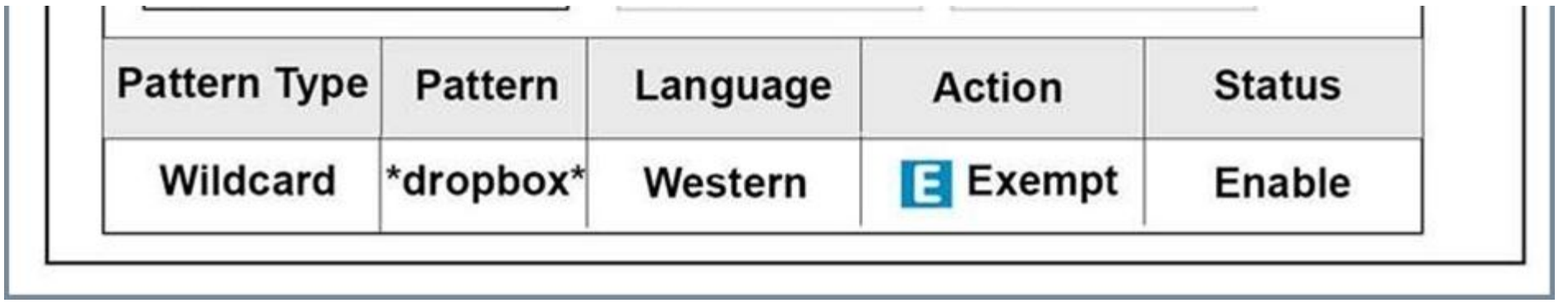
Create | Edit | Delete

URL	Type	Action	Status
*dropbox.com	Wildcard	Block	Enable

Web content filter

Create new | Edit | Delete

FORTINET
ipnshiken.com



Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	Exempt	Enable

ユーザーがファイル共有とストレージとして分類されているwww.dropbox.comにアクセスしようとした場合、FortiGateはどのアクションを実行しますか？

A. FortiGateは、Webコンテンツフィルタの設定に基づいて接続を免除します。

B. FortiGateは、URLフィルター設定に基づいて接続をブロックします。

C. FortiGateは、FortiGuardカテゴリベースのフィルタ設定に基づいた接続を許可します。

D. FortiGateは無効なURLとして接続をブロックします。

正解: **(**正解を表示します**)**

説明

fortigateは、静的URL-> FortiGuard->コンテンツ-詳細 java、Cookieの削除..）の順に実行するため、最初のステップでブロックします

質問: **61**

IBGPネットワークのBGPセッションの数を減らすために使用できる構成はどれですか。

A. 隣接範囲

B. ルートリフレクター

C. ネクストホップセルフ

D. 隣人グループ

正解: **(**正解を表示します**)**

ルートリフレクタは、AS内のIBGPセッションの数を減らすのに役立ちます。ルートリフレクタは、あるピアから学習したルータを他のピアに転送します。ルートリフレクタを設定する場合、フルメッシュのIBGPネットワークを作成する必要はありません。クラスタ内のすべてのクライアントは、同期ルーティングの更新を取得するためにリフレクタをルーティングするためだけにタルクします。ルートリフレクタは、AS内の他のルートリフレクタおよびボーダールータにルーティングアップデートを渡します。

有効的な**NSE7_EFW-6.4**問題集はJPNTest.com提供され、**NSE7_EFW-6.4**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE7_EFW-6.4**試験問題集を提供します。JPNTest.com NSE7_EFW-6.4試験問題集はもう更新されました。ここで**NSE7_EFW-6.4**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/NSE7_EFW-6.4-mondaishu　**124**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**

FortiGateが保存モードのときに、コンテンツ検査対象のトラフィックの動作を変更する2つの設定設定はどれですか。2つ選択してください。）

A. IPSフェイルオープン

B. AVフェイルオープン
C. UTMフェイルオープン
D. mem failopen
正解: **(**正解を表示します**)**

質問: **63**
FortiGateは、明らかな理由もなく予期せず再起動しています。管理者が問題に関する詳細情報を取得するために使用できるトラブルシューティングツールは何ですか？ 2つ選択してください。）
A. ログ。
B. クラッシュログ。
C. ファイアウォールモニター。
D. ポリシーモニター。
正解: **(**正解を表示します**)**

質問: **64**
デバッグコマンドの出力を含む展示を表示してから、以下の質問に答えてください。

```
# 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
```

このFortiGateに関する次の説明のうち正しいものはどれですか？
A. メモリ使用量が多いため、現在プロキシ保存モードになっています。
B. CPU使用率が高いため、現在システム保存モードになっています。
C. メモリ使用量が多いため、現在極端な保存モードになっています。
D. メモリ使用量が多いため、現在メモリ節約モードになっています。
正解: **(**正解を表示します**)**

質問: **65**
FortiGateデバイスには次のLDAP設定があります。

```
config user ldap
   edit "WindowsLDAP"
     set server "10.0.1.10"
     set cnid "cn"
     set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "dc=trainingAD, dc=training, dc=lab"
     set password xxxxxxx
   next
end
```

管理者は、WindowsLDAPサーバー10.0.1.10で「dsquery」コマンドを実行し、次の出力を取得しました。

> dsqueryユーザー-sami管理者
「CN =管理者、CN =ユーザー、DC =トレーニングAD、DC =トレーニング、DC =ラボ」
出力に基づいて、どのFortiGate LDAP設定が正しく構成されていませんか？
A. cnid。
B. ユーザー名。
C. パスワード。
D. dn。
正解: **B** (コメントを発表する)
https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516

質問: **66**
静的ルートがルーティングテーブルでアクティブになるには、次のどの条件が満たされる必要がありますか？ 3つ選択してください。）
A. 発信インターフェイスがアップしています。
B. ネクストホップIPアドレスは、発信インターフェイスサブネットの1つに属しています。
C. リンクヘルスモニター（構成されている場合）が起動しています。
D. 同じ目的地までの距離が長い他のルートはありません。
E. ネクストホップIPアドレスがアップしています。
正解: **A,B,C** (コメントを発表する)

質問: **67**
次のFortiGate設定を表示します。

```
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
```

jpnshiken.com

現在、インターネットへのすべてのトラフィックはポート1から出ています。展示では、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の部分的なセッション情報が表示されます。

```
# diagnose sys session list
session info: proto=6 proto_state+01 duration=17 expire=7 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic(bytes/packets/allow_err): org=57555/7/1 reply=23367/19/1 tuples=2
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)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

ルートID1の優先度が5から20に変更された場合、そのユーザーのセッションに一致するトラフィックはどうなりますか？

A. 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引き続きポート1から出力されます。

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

C. セッションはセッションテーブルに残り、そのトラフィックはポート2から出始めます。

D. セッションが削除されるため、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。

正解: **A** (コメントを発表する)

http://kb.fortinet.com/kb/documentLink.do?externalID=FD40943

質問: **68**

静的ルートがルーティングテーブルでアクティブになるには、次のどの条件が満たされる必要がありますか？ 3つ選択してください。）

A. ネクストホップIPアドレスがアップしています。

B. 同じ目的地までの距離が長い他のルートはありません。

C. リンクヘルスモニター（構成されている場合）が稼働しています。

D. ネクストホップIPアドレスは、発信インターフェイスサブネットの1つに属しています。

E. 発信インターフェイスがアップしています。

正解: (正解を表示します)

構成された静的ルートは、次のすべてが満たされた場合にのみ、ルーティングデータベースからルーティングテーブルに移動します。

発信インターフェイスがアップしています

距離が短い他の一致するルートはありません
リンクヘルスモニター（構成されている場合）は成功します
ネクストホップIPアドレスは、発信インターフェイスサブネットの1つに属しています

有効的な**NSE7_EFW-6.4**問題集はJPNTest.com提供され、**NSE7_EFW-6.4**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE7_EFW-6.4**試験問題集を提供します。JPNTest.com NSE7_EFW-6.4試験問題集はもう更新されました。ここで**NSE7_EFW-6.4**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/NSE7_EFW-6.4-mondaishu **124**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」