Fortinet.FCP_FGT_AD-7.6.v2026-08-10.q70

試験コード：	FCP_FGT_AD-7.6
試験名称：	FCP - FortiGate 7.6 Administrator
認証ベンダー：	Fortinet
無料問題の数：	70
バージョン：	v2026-08-10
ページの閲覧量：	106
問題集の閲覧量：	715

https://www.jpnshiken.com/shiken/Fortinet.FCP_FGT_AD-7.6.v2026-08-10.q70.html

質問: **1**
SD-WANのパフォーマンスSLAに関する記述のうち、正しいものはどれですか？ （3つ選択してください。）
A. セッション損失とジッターに依存しています。
B. それらは能動的にも受動的にも測定できます。
C. これらはSD-WANルールの最低コスト戦略に適用されます。
D. FortiGate デバイスの状態を監視します。
E. すべてのSLAターゲットを設定できます。
正解: **(**正解を表示します**)**
SD-WANのSLAは、パケット損失やジッターなどの指標を監視してリンク性能を評価します。SLAの測定は、アクティブプロービングまたはパッシブモニタリングを使用して実行できます。管理者は、すべてのSLAターゲットパラメータを設定して、パフォーマンス基準を定義できます。

質問: **2**
中間デバイスがIPsecトラフィックをブロックしているため、接続の問題が発生しています。
この問題を効果的に解決できる方法は、次のうちどれですか？ （2つ選択してください。）
A. SSL VPNトンネルモードを使用すると、ブロックされたESPおよびUDPポート（500または4500）の問題を回避できます。
B. SSL VPNトンネルを使用してハブアンドスポークトポロジを構成し、ブロックされたUDPポートをバイパスできます。
C. 大規模な証明書ネゴシエーションの問題を解決するために、フラグメンテーションを有効にすることができます。
D. IKEv2プロトコルを使用する必要があります。
正解: **A,B (**コメントを発表する**)**
このトレーニングの基本的な目的は、中間デバイスが原因で問題が発生する状況において、FortiGateのSSL VPNがIPSec VPNよりも優れている点を指摘することです。
IPsecはESPとUDP 500および4500を使用するため、これらがブロックされている場合、デフォルトでHTTPS（443）とTLS（両方ともTCP）を使用するSSL VPNトンネルモードが優れています。
UDPポートがブロックされている場合、SSL VPN（トンネルモードのハブアンドスポーク）はUDPを使用しないため、優れた性能を発揮します。

質問: **3**
FortiGateは、IPsec IKEv1認証のどの2つの機能をサポートしていますか？ （2つ選択してください。）
A. 拡張認証（XAuth）により、交換されるパケット数が少なくなり、認証が高速化されます。
B. 認証方法として事前共有鍵と証明書署名を使用する
C. 認証方法として証明書署名を設定する場合、リモートピアに証明書は必要ありません。
D. 拡張認証（XAuth）を使用して、リモートピアにユーザー名とパスワードの提供を要求します。

正解: **B,D** (コメントを発表する)
認証方法として事前共有鍵と証明書署名を使用する
FortiGateはIKEv1認証において事前共有鍵とデジタル証明書の両方をサポートしており、IPsec VPNトンネルのセキュリティ確保において柔軟性を提供します。
拡張認証 (XAuth) は、リモート ピアにユーザー名とパスワードの提供を要求するものです。FortiGate は IKEv1 で XAuth をサポートしており、ユーザー レベルの認証の追加レイヤーを追加できます。この場合、リモート ピアは IKE 認証情報に加えてユーザー名とパスワードを提供する必要があります。

質問: **4**
SSL証明書検査が有効になっている場合、FortiGateはSSLサーバーのホスト名を識別するために、どの3つの情報を使用しますか？ 3つ選択してください。）
A. HTTPヘッダーのホストフィールド。
B. クライアントハローメッセージのサーバー名表示（SNI）拡張機能
C. サーバー証明書のサブジェクト代替名（SAN）フィールド。
D. サーバー証明書の件名フィールド。
E. サーバー証明書のシリアル番号。
正解: **B,C,D** (コメントを発表する)
FortiGateデバイスでSSL証明書検査が有効になっている場合、システムは次の3つの情報を使用してSSLサーバーのホスト名を識別します。
* クライアントハローメッセージのサーバー名表示（SNI）拡張機能B） SNIは、SSL/TLSプロトコルのクライアントハローメッセージの拡張機能です。これは、クライアントが接続しようとしているホスト名を示します。これにより、FortiGateはSSLハンドシェイク中にサーバーのホスト名を識別できます。
* サーバー証明書のサブジェクト代替名（SAN）フィールド C）サーバー証明書のSANフィールドには、証明書が有効な追加のホスト名またはIPアドレスがリストされます。FortiGateはこのフィールドを検査して、サーバーのIDを確認します。
* サーバー証明書のサブジェクトフィールド D）サブジェクトフィールドには、証明書が発行されたプライマリホスト名またはドメイン名が含まれます。FortiGateはこの情報を使用して、SSL証明書の検査中にサーバーのIDを照合および検証します。
ホスト名識別のためのSSL証明書検査では、その他のオプションは使用されません。
* HTTP ヘッダーのホスト フィールド (A): これは HTTP リクエストの一部であり、SSL ハンドシェイクの一部ではないため、SSL 証明書の検査には使用されません。
* サーバー証明書のシリアル番号 (E): シリアル番号は証明書の管理と失効に使用され、ホスト名の識別には使用されません。
参考文献
* FortiOS 7.4.1 管理ガイド - SSL/SSH 検査、1802 ページ。
* FortiOS 7.4.1 管理ガイド - SSL/SSH 検査プロファイルの構成、1799 ページ。

質問: **5**
展示資料を参照してください。

HA configuration

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

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

HQ-NGFW-1 System Performance output

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

```
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

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

管理者は、HAクラスタのパフォーマンスステータス出力を55秒間監視しました。
プライマリのFortiGateはどれですか？
A. パラメータ memory-failover-threshold 設定の HQ-NGFW-2
B. パラメータ優先度設定付きHQ-NGFW-2
C. パラメータ memory-failover-flip-timeout 設定の HQ-NGFW-1
D. パラメータオーバーライド設定を備えたHQ-NGFW-1
正解: **(**正解を表示します**)**
HA構成ではオーバーライドが無効になっている（set override disable）と表示されますが、それにもかかわらず、HQ-NGFW-1は優先度が高く（200）、リソース使用量と稼働時間が高いことからプライマリとして動作しています。オーバーライド機能により、優先度の高いデバイスがプライマリとして動作を引き継ぐことができるため、HQ-NGFW-1がプライマリデバイスとなります。

質問: **6**
ネットワーク管理者は、2つのIPsec VPNトンネルと静的ルートを使用して、FortiGate上に冗長なIPsec VPNトンネルを設定したいと考えています。
両方のトンネルが稼働している場合、すべてのトラフィックはプライマリトンネルを経由してルーティングされる必要があります。セカンダリトンネルは、プライマリトンネルがダウンした場合にのみ使用されます。さらに、FortiGateはトンネルのダウンを検出して、トンネルのフェイルオーバーを高速化できる必要があります。
要件を満たすために、管理者はFortiGate上でどの2つの重要な設定変更を行う必要がありますか？（2つ選択してください。）
A. phase1-interfaceで、npu-offloadを有効にしてデッドトンネルを検出します。
B. プライマリトンネルの静的ルートの距離を短く設定し、セカンダリトンネルの静的ルートの距離を長く設定します。
C. デッドピア検出を有効にする。

D. VPNウィザードを使用して、冗長なIPsec VPNトンネル用のIPsecテンプレートを作成します。
正解: **B,C** (コメントを発表する)
プライマリトンネルのスタティックルートの距離を小さく設定し、セカンダリトンネルのスタティックルートの距離を大きく設定します。→ これにより、プライマリトンネルが常に優先され、セカンダリトンネルはプライマリルートが利用できない場合にのみ使用されるようになります。
デッドピア検出を有効にする → DPDを有効にすると、FortiGateはプライマリトンネルがダウンしたことを迅速に検出し、バックアップトンネルへのフェイルオーバーを高速化できます。

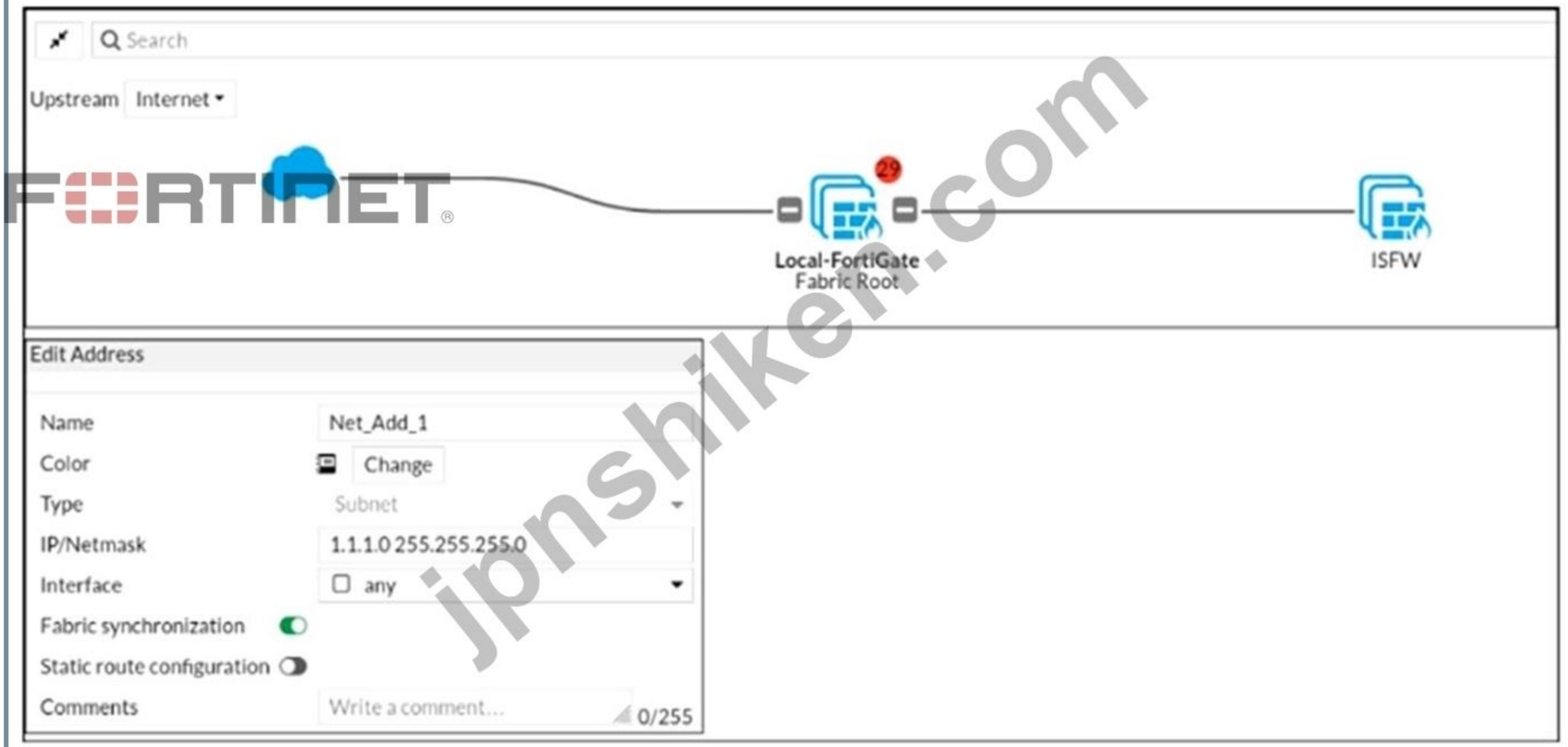
質問: **7**
添付の図を参照してください。この図は、リモート認証サーバーの構成の一部を示しています。

FortiGate管理者はこの設定をなぜ必要とするのですか？
A. RADIUSサーバーのシークレットを設定します。
B. FortiGateユーザーグループを認証する。
C. RADIUSサーバー上でトレーニングOUを認証し、照合します。
D. トレーニングユーザーグループのみを認証します。
正解: (正解を表示します)
Fortinet-Group-Name属性は、RADIUSサーバー上の『Training』ユーザーグループに所属するユーザーのみに認証を制限するために使用されます。

質問: **8**
FortiGateはFortiAnalyzerおよびFortiManagerと統合されています。
ファイアウォールポリシーを作成する際、FortiAnalyzerとFortiManagerの機能を強化し、ログ記録を有効にするために、管理者はどの属性を含める必要がありますか？
A. シーケンスID
B. ポリシーID
C. ログID
D. ユニバーサル一意識別子
正解: (正解を表示します)

質問: **9**
展示資料を参照してください。

Security Fabric physical topology view



Security Fabric configuration on Local-FortiGate

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream ''
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC Y9ynT+64RpCTpVdgSmoQHZ42mYSIzNNzLNvgzMXjyN
9hSjIJE3KYJlo3Xxyg1dvNxPId8T5xctBUszy7rgIcHcA/qHrByXSXfPEeHC6ufkqlPJr
W6GypwDUb5O3VFgPbASFYYteQesmwoJtGe84BLqa+hUcgunLDlz/97sBp+PLt5nrA==
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream "10.0.1.254"
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync local
end
ISFW #
```

管理者がセキュリティファブリック内のルートFortiGate（Local-FortiGate）上に新しいアドレスオブジェクトを作成します。同期後、このオブジェクトは下流のFortiGate（ISFW）では利用できません。
管理者はアドレスオブジェクトを同期するために何をする必要がありますか？

A. 両方のデバイスのcsfsettingを変更して、ダウンストリームアクセスを有効にします。

B. Local-FortiGate (root) の csfsetting を変更して、ファブリック オブジェクト統合のデフォルトを設定します。

C. ISFW (下流) の csfsetting を変更して、authorization-request-type certificate を設定します。

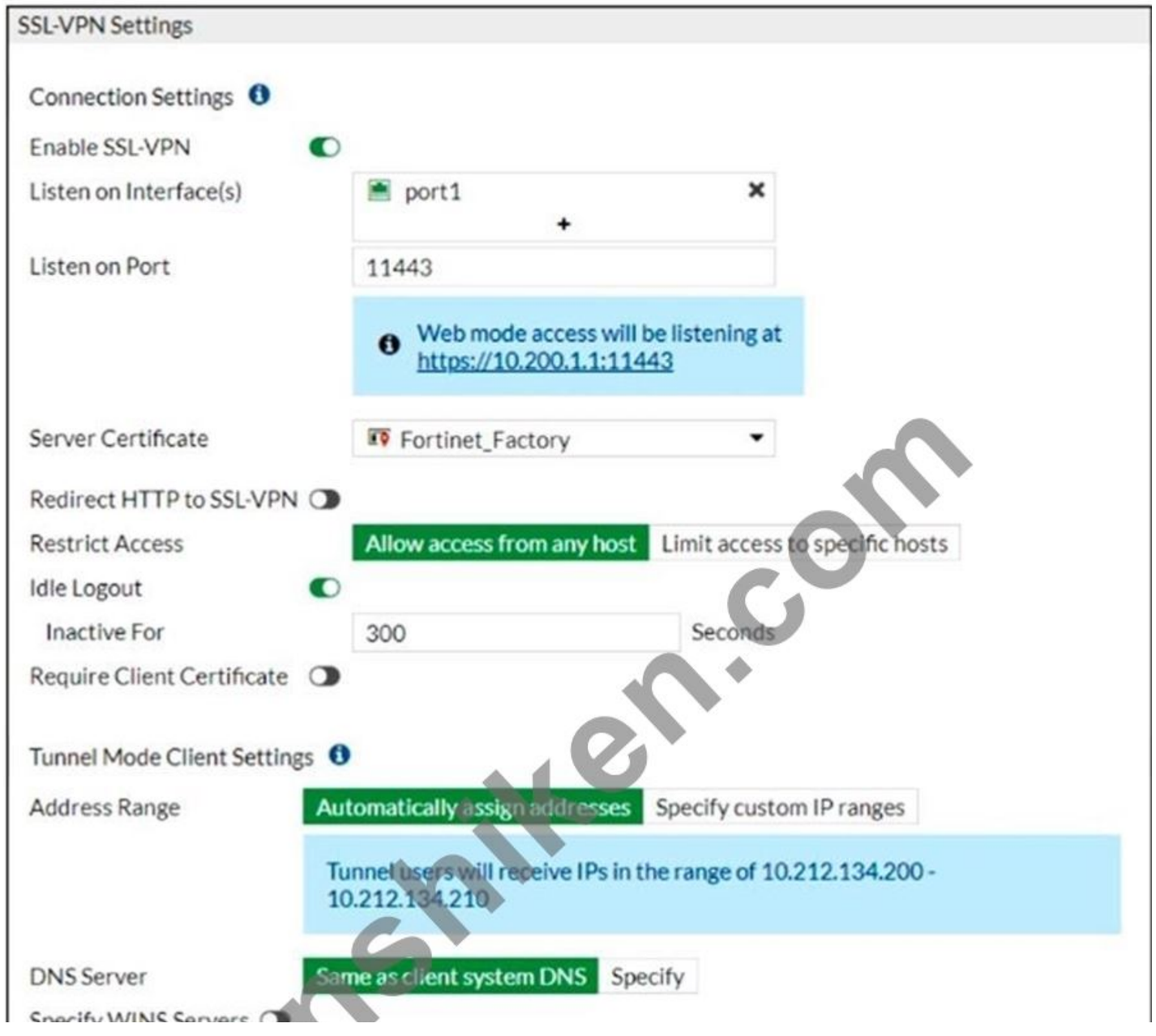
D. ISFW (下流) の csfsetting を変更して、configuration-sync local を設定します。

正解: **(**正解を表示します**)**

Fortinet Security Fabric の構成では、ルート FortiGate (ローカル FortiGate) が、アドレス オブジェクトなどの構成オブジェクトを下流の下位 FortiGate に同期します。
この同期を機能させるには、下流側のFortiGate（ISFW）のCSF（協調セキュリティファブリック）設定で、下流アクセスオプションが有効になっている必要があります。
展示内容：
ローカルFortiGateはダウンストリームアクセスが無効になっているため、設定をプッシュできません。

下流での変化。
ISFWにはダウンストリームアクセス無効化機能も備わっており、同期されたオブジェクトを受け入れることができません。
■
この問題を解決するには、設定の同期を可能にするために、両方のFortiGateでダウンストリームアクセスを有効にする必要があります。

質問: **10**
展示資料を参照してください。
SSL-VPN settings



ユーザーがSSL VPNに接続しようとすると、接続が失敗します。
ユーザーがSSL VPNに正常に接続するには、どのような操作を行うべきですか？
A. クライアントのSSL VPNポートを変更します。
B. SSL VPN ポータルをトンネルに変更します。

C. サーバーのIPアドレスを変更します。
D. アイドルタイムアウトを変更します。
正解: **(**正解を表示します**)**
FortiGate SSL-VPN 設定では、VPN はポート 11443 でリッスンするように構成されています。
ポートでリッスン」フィールド。しかし、VPNクライアントは、設定されたポートではなく、デフォルトのHTTPSポート 443）を使用するhttps://10.200.1.1:443/に接続しようとしています。
接続を正常に行うには、クライアント側のSSL VPNポートを11443に変更し、FortiGateデバイスで定義されているリスニングポートと一致させる必要があります。

質問: **11**
図を参照してください。管理者としてIPSプロファイルを作成しましたが、期待どおりに動作していません。テスト中に、図に示すような出力が得られました。
展示されている診断結果の考えられる原因は何でしょうか？

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
            pid = 2044, engine count = 0 (+1)
            0 - pid:2074:2074 cfg:1 master:0 run:1
```

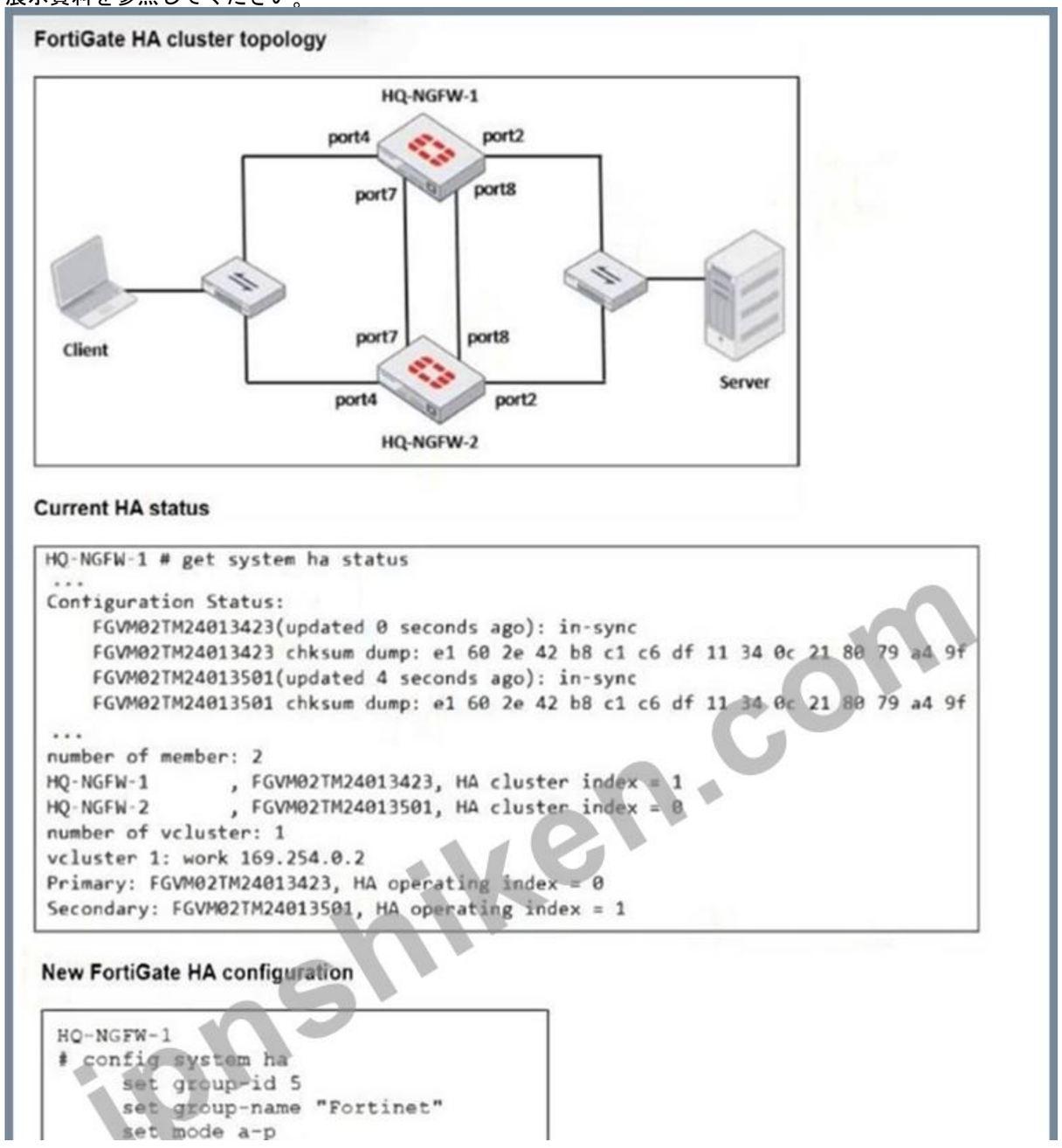
A. IPSセキュリティプロファイルが設定されたファイアウォールポリシーがありません。
B. FortiGateがIPS障害オープン状態になりました。
C. 管理者がコマンド diagnose test application ipsmonitor 5 を入力しました。
D. 管理者がコマンド diagnose test application ipsmonitor 99 を入力しました。
正解: **A** (コメントを発表する)
出力結果にはIPSエンジン数が0と表示されており、アクティブなIPSエンジンが実行されていないことを示しています。これは通常、ファイアウォールポリシーがIPSセキュリティプロファイルを参照していないことを意味し、そのためIPSプロファイルが適用されず、トリガーもされていません。

質問: **12**
FortiGateはFortiAnalyzerおよびFortiManagerと統合されています。
ファイアウォールポリシーを作成する際、FortiAnalyzerとFortiManagerの機能を強化し、ログ記録を有効にするために、管理者はどの属性を含める必要がありますか？
A. ポリシーID
B. ログID
C. ユニバーサルー意識別子
D. シーケンスID
正解: **(**正解を表示します**)**
FortiGateは、各ファイアウォールポリシーに一意の識別子（UUID）を使用します。このUUIDはFortiAnalyzerおよびFortiManagerと同期されるため、ポリシーIDやシーケンスが変更された場合でも、これらのツールはポリシーを確実に識別できます。これにより、統合されたデバイス全体で一貫したログ記録と機能強化が保証されます。

質問: **13**
自動縫製の特徴として正しい記述はどれですか？
A. トリガーは1つ以上持つことができます。
B. これらはファブリック内の下流デバイスでのみ作成できます。
C. 複数のアクションを同時に実行できます。

D. セキュリティファブリック内のデバイスでのみ実行できます。
正解: **(**正解を表示します**)**
FortiGateのオートメーションステッチは、1つ以上のトリガーと1つ以上のアクションを含むイベント駆動型のワークフローです。トリガーはステッチを開始する条件（ログイン失敗やシステムイベントなど）を定義し、アクションはFortiGateがそれに応じて実行すべき処理（アラートの送信やスクリプトの実行など）を定義します。

質問: **14**
展示資料を参照してください。

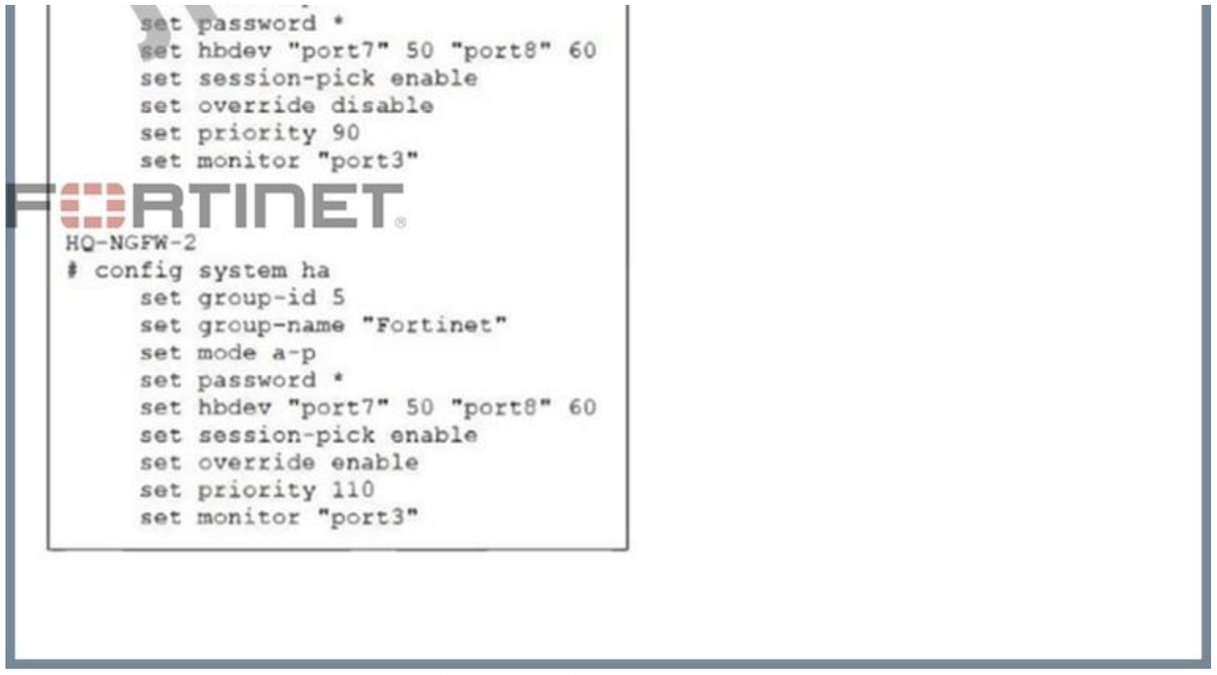


Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
    FGVM02TM24013423(updated 0 seconds ago): in-sync
    FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
    FGVM02TM24013501(updated 4 seconds ago): in-sync
    FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1       , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2       , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1
```

New FortiGate HA configuration

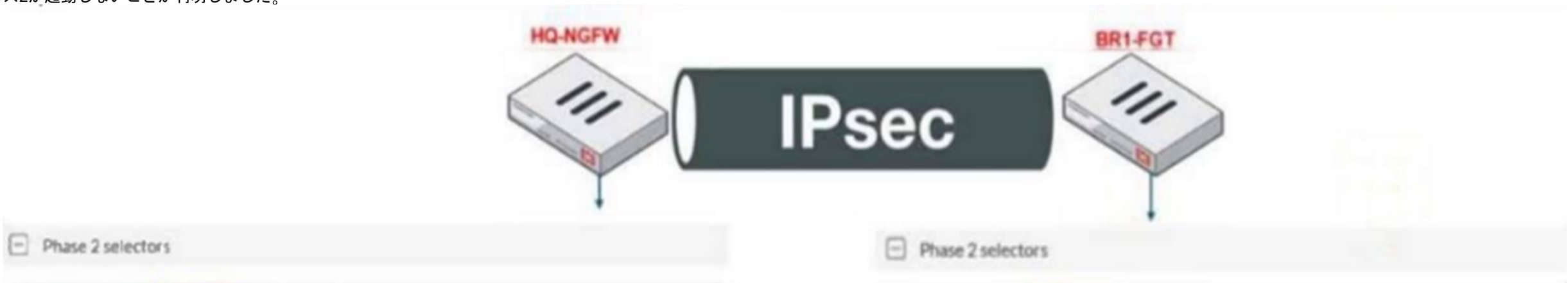
```
HQ-NGFW-1
# config system ha
    set group-id 5
    set group-name "Fortinet"
    set mode a-p
```

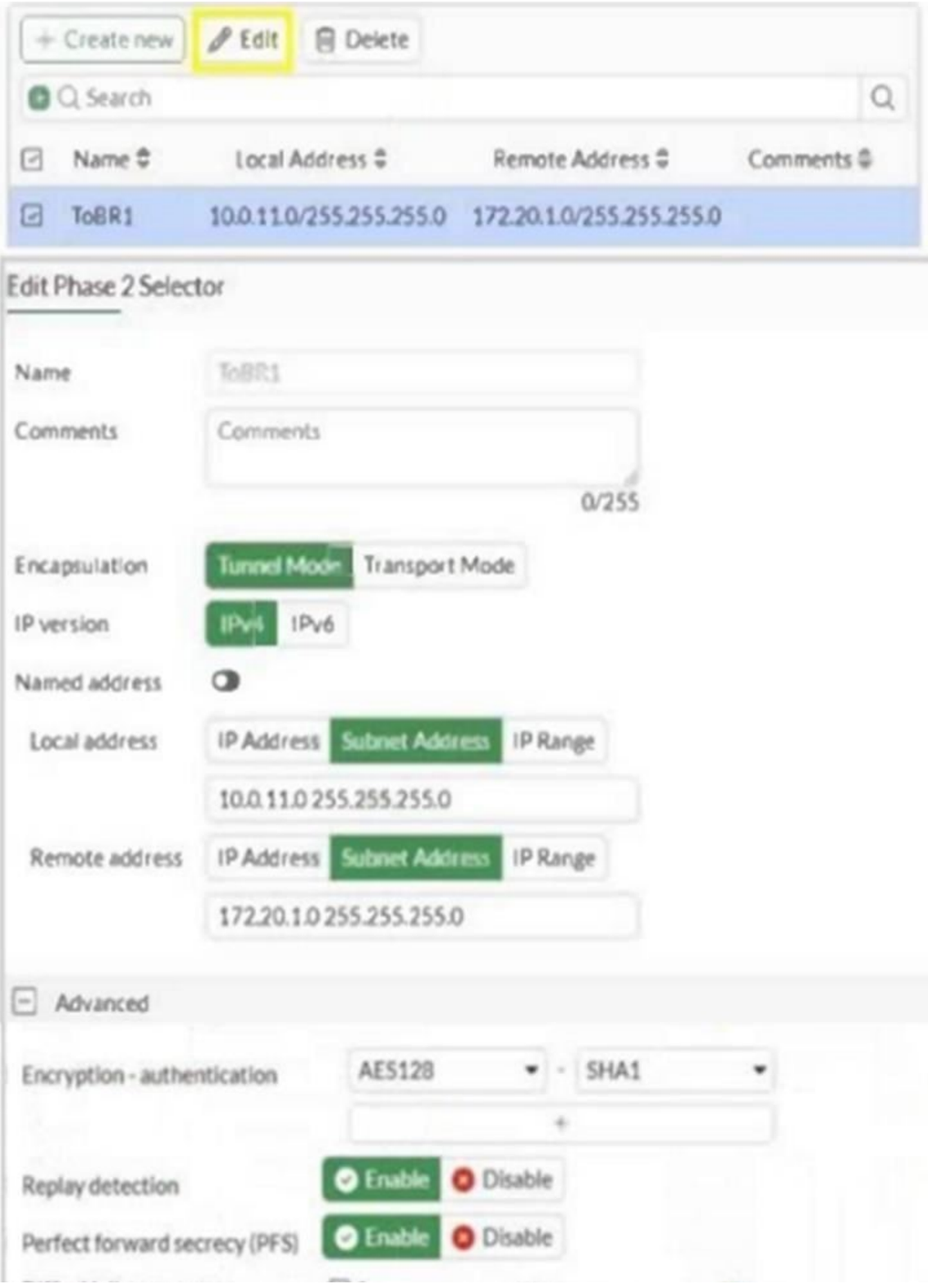


現在のHAステータスに基づいて、管理者は図に示すように、HQ-NGFW-1とHQ-NGFW-2のオーバーライドおよび優先度パラメータを更新します。
HAクラスターではどのような結果が予想されるでしょうか？

A. HQ-NGFW-1 はオーバーライド無効化設定を HQ-NGFW-2 と同期します。
B. HQ-NGFW-2 はオーバーライド有効化設定を持ち、HQ-NGFW-1 よりも優先度が高いため、プライマリとして引き継ぎます。
C. HQ-NGFW-2の優先度が低いため、HQ-NGFW-1がプライマリのままになります。
D. HA クラスターは同期が取れなくなります。オーバーライド設定はすべての HA メンバーで一致する必要があるためです。
正解: **(**正解を表示します**)**
HQ-NGFW-2でオーバーライドが有効になっており、優先度が高い（10対90）ため、HQ-NGFW-2がプライマリデバイスとなり、現在のプライマリステータスに関わらず、HQ-NGFW-1を優先します。

質問: **15**
図を参照してください。ネットワーク管理者が、2台のFortiGateデバイス間のIPsecトンネルのトラブルシューティングを行っています。管理者は、フェーズ1の状態は正常であることを確認しましたが、フェーズ2が起動しないことが判明しました。




Create new
Edit
Delete
Search
Name
Local Address
Remote Address
Comments
ToBR1
10.0.11.0/255.255.255.0
172.20.1.0/255.255.255.0
Edit Phase 2 Selector
Name
ToBR1
Comments
Comments
0/255
Encapsulation
Tunnel Mode
Transport Mode
IP version
IPv4
IPv6
Named address
Local address
IP Address
Subnet Address
IP Range
10.0.11.0 255.255.255.0
Remote address
IP Address
Subnet Address
IP Range
172.20.1.0 255.255.255.0
Advanced
Encryption - authentication
AES128
SHA1
Replay detection
Enable
Disable
Perfect forward secrecy (PFS)
Enable
Disable


Create new
Edit
Delete
Search
Name
Local Address
Remote Address
Comments
ToHQ
172.20.1.0/255.255.255.0
10.11.0.0/255.255.255.0
Edit Phase 2 Selector
Name
ToHQ
Comments
Comments
0/255
Encapsulation
Tunnel Mode
Transport Mode
IP version
IPv4
IPv6
Named address
Local address
IP Address
Subnet Address
IP Range
172.20.1.0 255.255.255.0
Remote address
IP Address
Subnet Address
IP Range
10.11.0.0 255.255.255.0
Advanced
Encryption - authentication
AES256
SHA1
Replay detection
Enable
Disable
Perfect forward secrecy (PFS)
Enable
Disable

図に示されているフェーズ2の構成に基づくと、フェーズ2を起動させるには、どの2つの構成変更が必要ですか？ 2つ選択してください。）

A. BR1-FGTで、秒数を43200に設定します。

B. HQ-NGFWで、Diffie-Hellmanグループ2を有効にします。

C. BR1-FGTで、リモートアドレスを10.0.11.0/255.255.255.0に設定します。

D. HQ-NGFW で暗号化を AES256 に設定します。

正解: **(**正解を表示します**)**

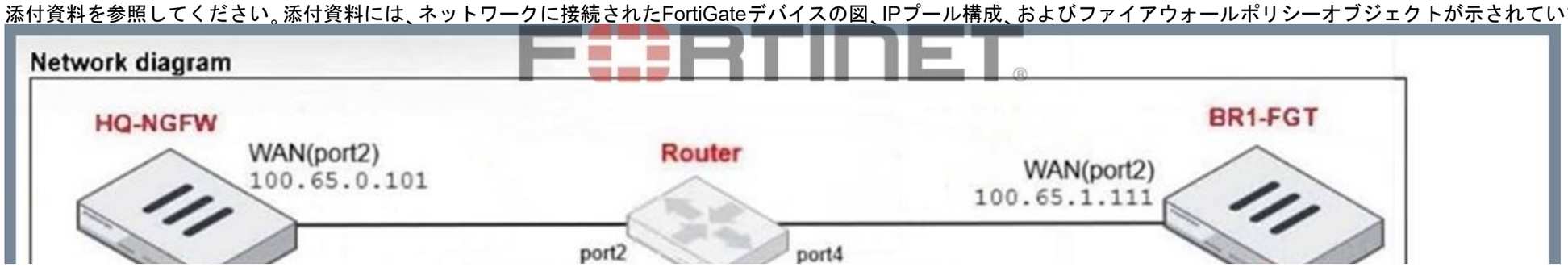
キーの有効期間（秒は両側で一致する必要があります。BR1-FGT は 14400 に設定されているため、

43200件がHQ-NGFWに一致しました。

BR1-FGTのリモートアドレスは、HQ-NGFWのローカルサブネット（10.0.11.0/24）と一致させる必要がありますが、現在は172.20.1.0/24と誤って設定されています。これを10.0.11.0/255.255.255.0に変更することで、フェーズ2セレクタが正しく動作します。

質問: **16**

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



NAT IP pool configuration

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

Firewall policies

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

WAN（ポート2）インターフェースのIPアドレスは100.65.0.101/24です。LAN（ポート4）インターフェースのIPアドレスは10.0.11.254/24です。HQ-PC-1（10.0.11.50）のユーザーがBR-FGT（100.65.1.111）のIPアドレスにpingを実行する場合、トラフィックのソースNAT（SNAT）にはどちらのIPアドレスが使用されますか？

A. 100.65.0.101
B. 100.65.0.49
C. 100.65.0.99
D. 100.65.0.149

正解: (正解を表示します)
pingトラフィックポリシーは、外部IP範囲を持つSNAT-Remote1という名前のIPプールを使用します。
100.65.0.99。したがって、このポリシーに一致するトラフィック（HQ-PC-1 から BR1-FGT への ping）は、
ソースNATは100.65.0.99です。

質問: **17**
図を参照してください。管理者が静的ルートの宛先として使用する新しいファイアウォールアドレスを作成しました。管理者が新しい静的ルートの宛先フィールドで新しいアドレスを選択できないのはなぜですか？

A. 新しい静的ルートでは、管理者は名前付きアドレスを選択する必要があります。
B. 新しいファイアウォールアドレスでは、まずFQDNアドレスを解決する必要があります。
C. 新しい静的ルートでは、管理者はまずインターフェースをポート2に設定する必要があります。
D. 新しいファイアウォールアドレスでは、ルーティング設定を有効にする必要があります。
正解: (正解を表示します)
静的ルートの宛先としてFQDNベースのアドレスオブジェクトを使用するには、ファイアウォールのアドレス設定で 『ルーティング設定」オプションを有効にする必要があります。これを有効にしないと、そのアドレスをルーティング対象として選択できません。

質問: **18**

展示資料を参照してください。

管理者は、Facebookを除くすべてのソーシャルネットワーキングサイトへのアクセスをブロックするようにWebフィルタプロファイルを設定しました。しかし、ユーザーがFacebook.comにアクセスしようとすると、FortiGuardのWebフィルタリングブロックページにリダイレクトされます。

提示された資料に基づき、管理者はFacebookへのアクセスを許可しつつ、他のすべてのソーシャルネットワーキングサイトをブロックするために、どのような設定変更を行う必要がありますか？

A. 静的URLフィルタセクションでタイプをシンプルに変更します。

B. FortiGuard カテゴリベースフィルタでソーシャルネットワーキングのアクションを警告に設定します。

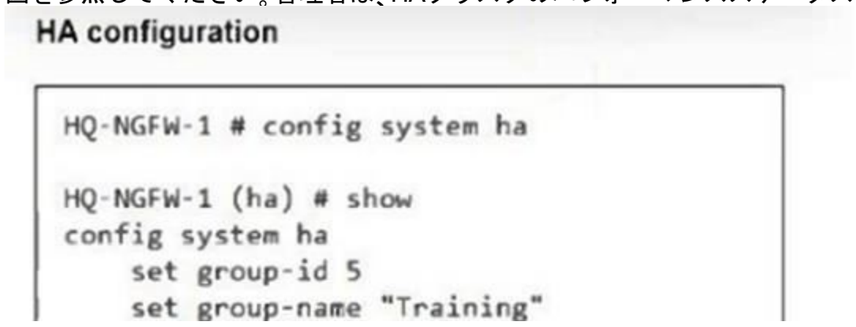
C. Webフィルタプロファイルの機能セットをプロキシベースに変更します。

D. 静的URLフィルタで、www.facebook.comのアクションを 除外」に設定します。

正解: **D** (コメントを発表する)

質問: **19**

図を参照してください。管理者は、HAクラスタのパフォーマンスステータス出力を55秒間監視しました。



```
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

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

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
```

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

プライマリのFortiGateはどれですか？

A. パラメータ memory-failover-threshold 設定の HQ-NGFW-2

B. パラメータ優先度設定付きHQ-NGFW-2

C. パラメータ memory-failover-flip-timeout 設定の HQ-NGFW-1

D. パラメータオーバーライド設定を備えたHQ-NGFW-1

正解: **(**正解を表示します**)**

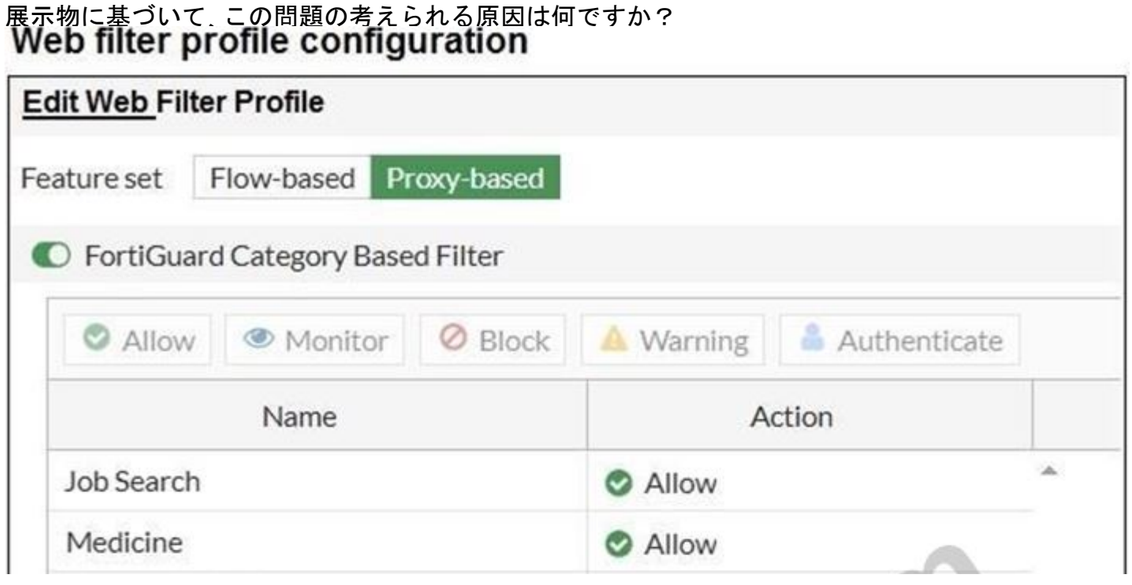
HA構成ではオーバーライドが無効になっている（set override disable）と表示されますが、それにもかかわらず、HQ-NGFW-1は優先度が高く（200）、リソース使用量と稼働時間が高いことからプライマリとして動作しています。オーバーライドは優先度の高いデバイスがプライマリとして動作することを許可するため、HQ-NGFW-1がプライマリデバイスとなります。

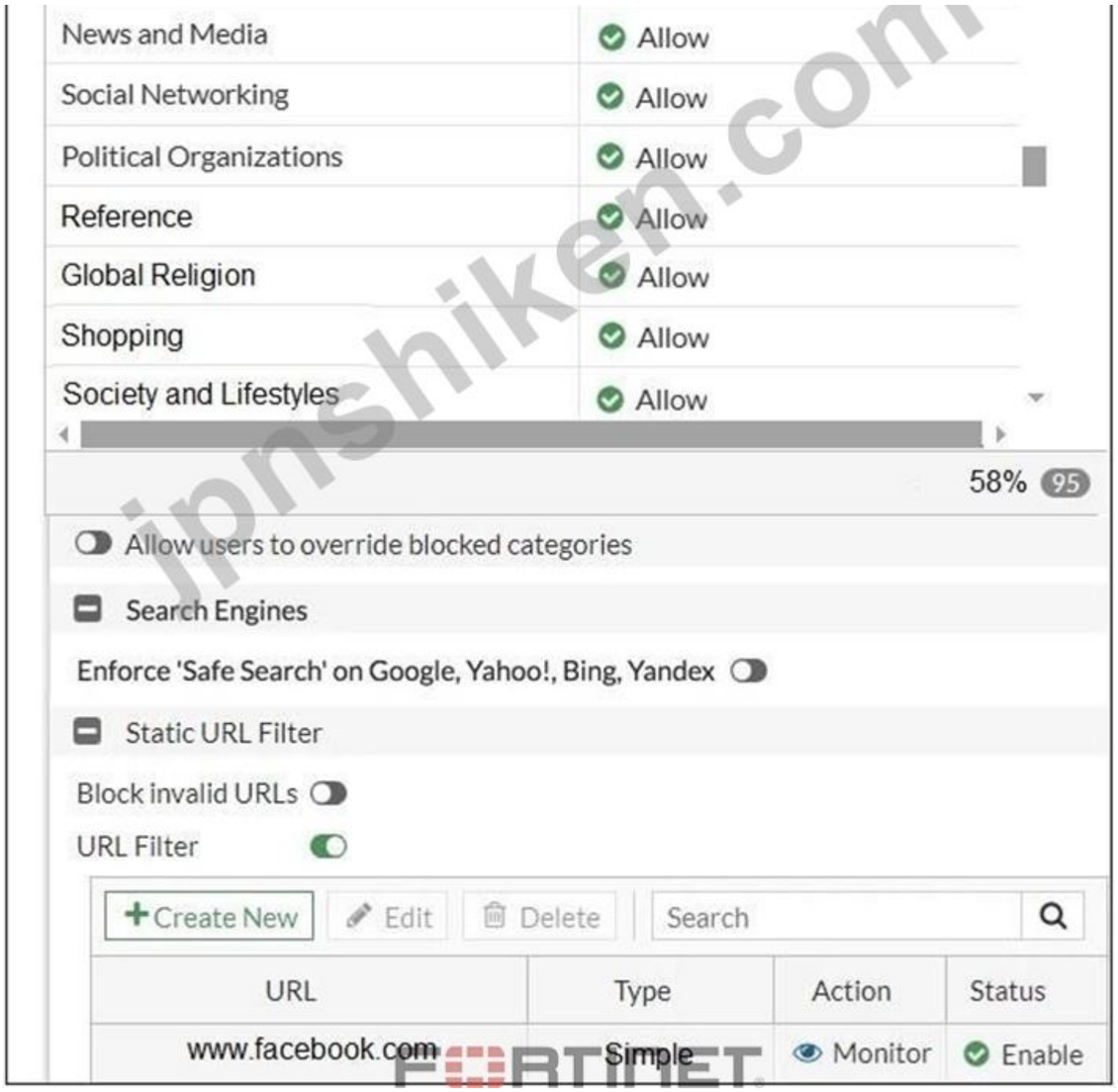
質問: **20**

図を参照してください。ウェブフィルタプロファイルの設定とファイアウォールポリシーの設定が示されています。

あなたはwww.facebook.comにアクセスしようとしていますが、FortiGuardのWebフィルタリングブロックページにリダイレクトされています。

展示物に基づいて、この問題の考えられる原因は何ですか？





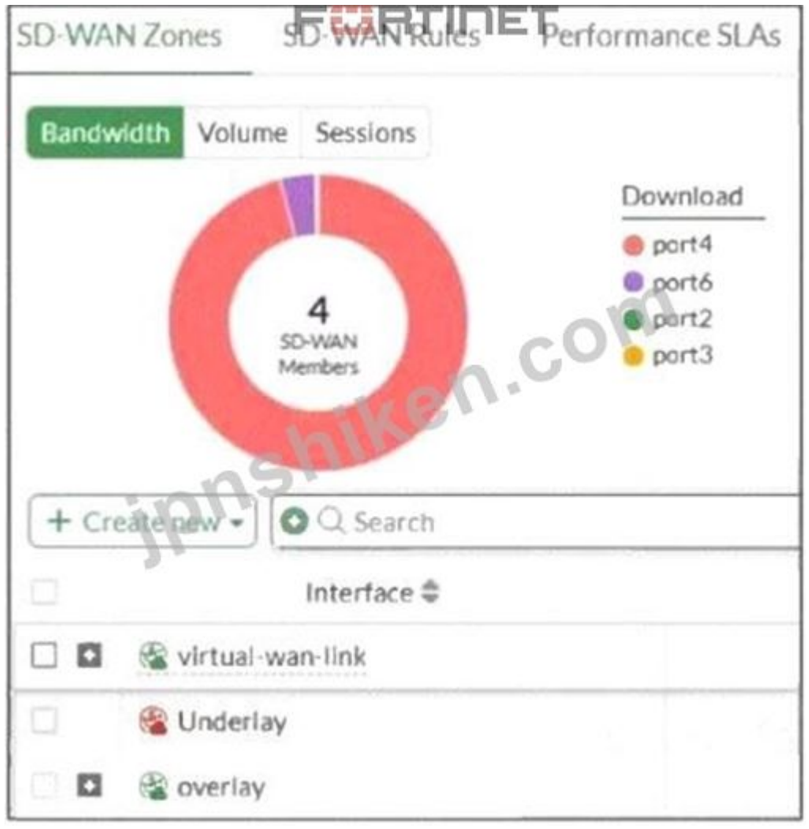
FortiGuard block page

A. ウェブフィルタプロファイル機能セットの設定が正しくありません。
B. Webレーティングの上書き設定が間違っています。
C. ファイアウォールポリシーの検査モードが正しくありません。
D. www.facebook.com の場合、URL フィルタの動作が正しくありません。
正解: **(**正解を表示します**)**
ウェブフィルタプロファイルには、www.facebook.com に対する URL フィルタのオーバーライドが設定されており、アクションは 監視」となっています。これによりアクセスが許可されるはずです。しかし、ブロックページでは FortiGuard が www.facebook.com を悪意のある Web サイトとして分類し、ブロックしていることが示されています。これは、ウェブ評価のオーバーライド設定が正しくない オーバーライドが正しく適用されていない）ため、FortiGuard のデフォルトのカテゴリアクションが優先され、サイトがブロックされていることを示しています。

質問: **21**
ファイアウォールポリシーを設定する際、ポリシーIDに関して次のうちどれが正しいですか？
A. GUIまたはCLIに関係なく、ファイアウォールポリシーを作成する際にはポリシーIDを指定することが必須です。
B. ファイアウォールポリシーIDは、ファイアウォールポリシーにおけるポリシーの実行順序を識別します。
C. CLIでポリシーID 0のポリシーを作成できます。

D. ポリシーが作成されると、ポリシーIDは編集できません。
正解: (正解を表示します)
ファイアウォールポリシーが作成されると、そのポリシーIDは固定され、変更することはできません。このIDは、FortiGateの設定内でポリシーを一意に識別するものです。

質問: **22**
FortiGateのGUI上でのSD-WANゾーン構成を示す図を参照してください。

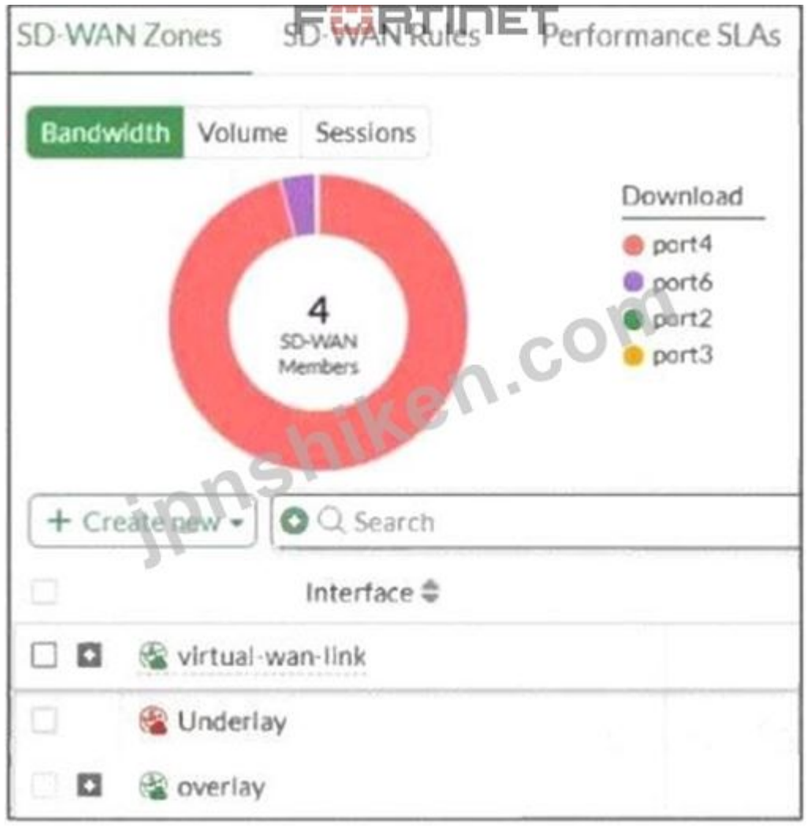


展示内容に基づくと、次のうち正しい記述はどれですか？
A. アンダーレイゾーンはデフォルトのゾーンです。
B. アンダーレイゾーンには部材がありません。
C. ポート2とポート3はゾーンに割り当てられていません。
D. 仮想WANリンクとオーバーレイゾーンを削除できます。
正解: (正解を表示します)
アンダーレイゾーンはデフォルトのSD-WANゾーンであり、通常はオーバーレイリンクや仮想リンクが追加される前のSD-WAN構成における物理インターフェースを表します。

質問: **23**
SSL VPN環境において、中間デバイスがトラフィックをブロックすることによって引き起こされる接続問題を分析しています。
この問題を効果的に解決できる方法は、次のうちどれですか？ 2つ選択してください。）
A. IKEフラグメンテーションを無効にすることで、大規模な証明書ネゴシエーションの問題を解決できます。
B. フラグメントドロップや大規模な証明書交換の問題を解決するには、IPsecを使用する必要があります。

C. SSL VPNトンネルモードを使用すると、ブロックされたESPおよびUDPポート 500または4500）の問題を回避できます。
D. ハブアンドスポークトポロジーをSSL VPNトンネルで構成して、ブロックされたUDPポートをバイパスできます。
正解: (正解を表示します)
IKEフラグメンテーションを無効にすることで、証明書交渉中に中間デバイスが大きな断片化されたパケットをブロックすることによって発生する問題を解決できます。
SSL VPNトンネルモードを使用すると、トラフィックがHTTPS経由でカプセル化され、IPsecで一般的に使用されるESPポートとUDPポートのブロックを回避できます。

質問: **24**
FortiGateのGUI上でのSD-WANゾーン構成を示す図を参照してください。



展示内容に基づくと、次のうち正しい記述はどれですか？
A. アンダーレイゾーンはデフォルトのゾーンです。
B. アンダーレイゾーンには部材がありません。
C. ポート2とポート3はゾーンに割り当てられていません。
D. 仮想WANリンクとオーバーレイゾーンを削除できます。
正解: (正解を表示します)
アンダーレイゾーンはデフォルトのSD-WANゾーンであり、通常はオーバーレイリンクや仮想リンクが追加される前のSD-WAN構成における物理インターフェースを表します。

質問: **25**
コレクターエージェントがADポーリングに使用する3つの方法はどれですか？ 3つ選択してください。）
A. WinSecLog

B. NetAPI
C. FortiGateポーリング
D. FSSO REST API
E. WMI
正解: **(**正解を表示します**)**
Fortinet Collector Agent は、以下の方法を使用して Active Directory (AD) からユーザーログオンイベントをポーリングできます。
NetAPI - ドメインコントローラーに直接クエリを実行して、ユーザーのログオン情報を取得します。
■
FSSO REST API - 最新のAPIベースの通信を介してユーザーとの統合とポーリングを可能にします
■
認証情報の更新。
WMI（Windows Management Instrumentation）- ドメインコントローラーからログオンデータを取得します。
■
WMIクエリを使用する。

質問: **26**
自動化ステッチの特徴を説明しているのは、次のうちどれですか？（2つ選択してください。）
A. トリガーには外部コネクタが関与する場合があります。
B. 自動ステッチには複数のトリガーを設定できます。
C. アクションは、セキュリティファブリックに含まれるデバイスのみを対象とします。
D. 複数のアクションを並行して実行できます。
正解: **(**正解を表示します**)**

質問: **27**
ネットワーク管理者が、インターフェースペアビューとシーケンスビューの両方でファイアウォールポリシーを確認している。
各ビューでは、ポリシーの表示順序が異なります。
この2つの見解において、政策順序が異なるのはなぜか？
A. インターフェースペアビューのポリシーはセキュリティレベルによって優先順位が付けられますが、シーケンスビューでは管理者の手動による順序付けが厳密に適用されます。
B. シーケンスビューではルールの優先順位に基づいてポリシーをグループ化しますが、インターフェースペアビューは常にトラフィックログの順序に従います。
C. ファイアウォールは、最近のトラフィックパターンに基づいてインターフェイスペアビューのポリシーを動的に再編成しますが、シーケンスビューは静的なままです。
D. インターフェースペアビューは、一致するインターフェースに基づいてポリシーをソートし、シーケンスビューはルールの実際の処理順序を表示します。
正解: **(**正解を表示します**)**
インターフェイスペアビューでは、ポリシーが送信元インターフェイスと宛先インターフェイスごとにグループ化されて表示されますが、シーケンスビューでは、ファイアウォールによって処理される正確な順序でポリシーが表示されます。

質問: **28**
FortiGate上で以下のコマンドを設定しました。

```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

この構成はFortiGateにどのような影響を与えるでしょうか？

A. FortiGate はすべてのインターフェースで厳格な RPF を有効にし、ポート 1 は非対称ルーティングを有効にします。

B. FortiGate はすべてのインターフェースで厳格な RPF を有効にし、ポート 1 は RPF チェックから除外されます。

C. ポート1はフレキシブルRPFが有効になり、その他のすべてのインターフェースは厳密RPFが有効になります。

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

正解: **B (**コメントを発表する**)**

グローバル設定では、デフォルトで全てのインターフェースで厳密なソースコードチェック（RPF）が有効になります。インターフェースごとの設定では、ポート1のソースコードチェックが無効になり、厳密なRPFの適用対象から除外されます。

質問: **29**

図を参照してください。SD-WANは、SD-WANルールに一致しないトラフィックを分散するために、どのアルゴリズムを使用しますか？

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

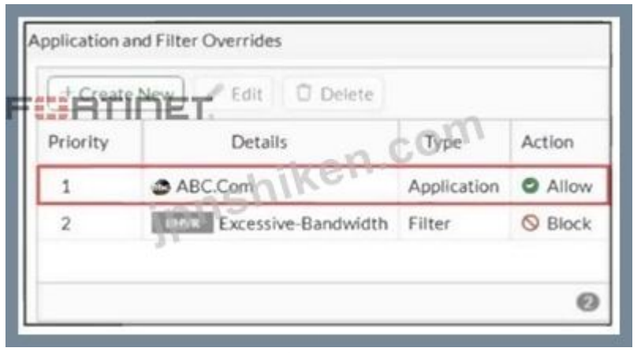
A. 送信元IPから宛先IPへのすべてのトラフィックは、同じインターフェースに送信されます。

B. トラフィックは、レイテンシが最も低いリンクに送信されます。

C. トラフィックは、各インターフェースを通過するセッション数に基づいて分散されます。

D. 送信元IPアドレスからのすべてのトラフィックは同じインターフェースに送信されます
正解: **A** (コメントを発表する)
定義されたSD-SWANルールに一致しないトラフィックについては、デフォルトの暗黙的なSD-WANルールが適用されます。デフォルトでは、FortiGateは 送信元IPアドレスと宛先IPアドレスに基づく」アルゴリズムを使用します。つまり、特定の送信元IPアドレスから特定の宛先IPアドレスへのすべてのトラフィックは、同じインターフェースを経由して送信されます。
これにより、同じ送信元IPアドレスと宛先IPアドレス間のトラフィックに対して、一貫した経路が使用されることが保証されます。

質問: **30**
展示資料を参照してください。



管理者は、ABC.Com アプリケーション署名に対してアプリケーションオーバーライドを設定し、アクションを 許可」に設定しました。このアプリケーション制御プロファイルは、すべての送信トラフィックをスキャンするファイアウォールポリシーに適用されます。ファイアウォールポリシーではログ記録が有効になっています。設定をテストするために、管理者は ABC.Com Web サイトへ複数回アクセスしました。
ABC.Comのセキュリティログにログが生成されないのはなぜですか？
A. ABC.Com タイプがフィルターではなくアプリケーションに設定されています。
B. ABC.Com はアプリケーション プロファイルで構成されており、Web フィルタ プロファイルとして構成する必要があります。
C. ABC.Com のアクションは 許可」に設定されています。
D. ABC.Com は 帯域幅過剰」のカテゴリに該当します。
正解: (正解を表示します)
アプリケーションのオーバーライドでアクションが 許可」に設定されている場合、このオーバーライドに一致するトラフィックは、より詳細な検査やブロックをバイパスするため、セキュリティログを生成することなく許可されます。

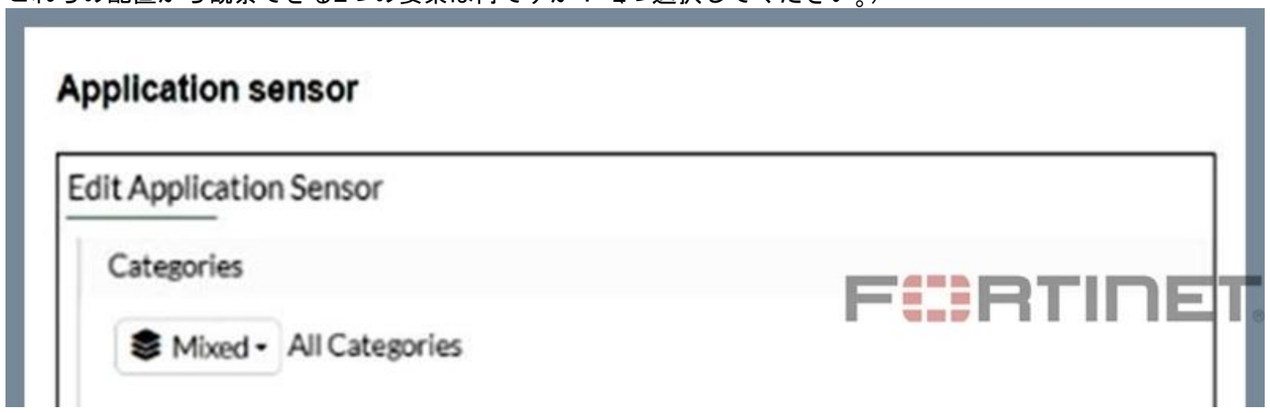
質問: **31**
図を参照してください。管理者はSD-WANルールを設定し、FortiGateのトラフィックログページにSD-WAN固有の列 $D-WAN品質とSD-WANルール名）を表示するように設定しました。
FortiGateは、最上位に設定されているポリシーID 1に従ってトラフィックを許可します。これはSD-WANトラフィックを許可するポリシーです。しかし、これらの設定にもかかわらず、トラフィックログには、これらのトラフィックフローを制御するために使用されたSD-WANルールの名前が表示されません。
原因は何だろうか？

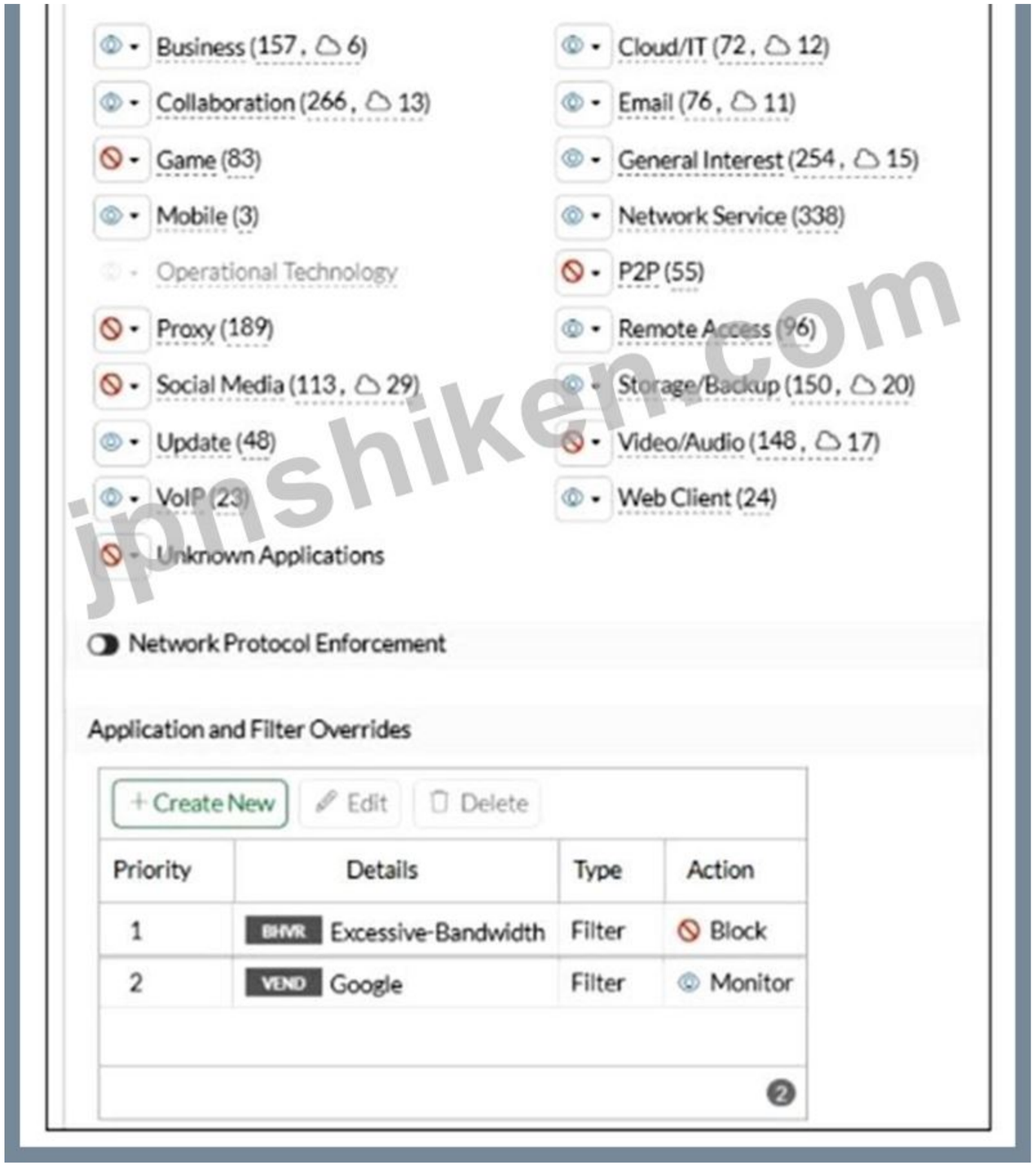
SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	Accept (8.08 kB / 27…	1(DIA)	port2		
YouTube	Accept (UTM Allowed)	1(DIA)	port2		
Facebook	Accept (UTM Allowed)	1(DIA)	port1		
Facebook	Accept (UTM Allowed)	1(DIA)	port1		
Facebook	Accept (3.33 kB / 10…	1(DIA)	port1		
YouTube	Accept (44.63 kB/ 3…	1(DIA)	port2		
CNN	Accept (UTM Allowed)	1(DIA)	port1		
CNN	Accept (UTM Allowed)	1(DIA)	port2		
CNN	Accept (UTM Allowed)	1(DIA)	port2		

A. SD-WANルール名はすぐには表示されません。管理者はページを更新する必要があります。
B. ファイアウォールポリシーにアプリケーション制御プロファイルが適用されていません。
C. FortiGateは暗黙のSD-WANルールに従ってトラフィックの負荷分散を行いました。
D. SD-WANルール内の宛先はアプリケーションごとに構成されていますが、機能の可視性は有効になっていません。
正解: **(**正解を表示します**)**
SD-WANトラフィックログには、トラフィックが暗黙のSD-WANルールによって転送されているため、SD-WANルール名は表示されません。明示的なSD-WANルールがトラフィックに一致しない場合、FortiGateはデフォルトの暗黙ルールにフォールバックし、設定された戦略（ボリュームやセッションなど）に基づいてトラフィックのバランスを取ります。明示的なルールが適用されないため、ログのルール名フィールドは空白のままになります。

質問: **32**
添付資料を参照してください。添付資料に示すように、アプリケーションセンサーとそれに対応するファイアウォールポリシーを実装済みです。
これらの配置から観察できる2つの要素は何ですか？ 2つ選択してください。）





A. YouTube検索は、Googleアプリケーションとフィルタの上書き設定に基づいて許可されます。
B. YouTubeへのアクセスは、帯域幅超過アプリケーションおよびフィルタオーバーライド設定に基づいてブロックされています。
C. Facebookへのアクセスは許可されていますが、動画/音声カテゴリのフィルタ設定により、Facebookの動画を再生することはできません。
D. カテゴリフィルター設定に基づき、Facebookへのアクセスがブロックされています。
正解: **(**正解を表示します**)**
Facebookはソーシャルメディアアプリのカテゴリに属しており、アプリセンサーではこのカテゴリが 「ブロック」に設定されています。そのため、Facebookアプリからのトラフィックはすべてカテゴリによってブロックされます。
帯域幅超過動作フィルタは、優先度1、アクション 「ブロック」のオーバーライドとして設定されています。YouTubeストリーミングアプリケーションには帯域幅超過動作のタグが付けられているため、このオー

バーライドはGoogle（ベンダー）の監視ルールよりも優先され、結果としてYouTubeがブロックされます。

質問: **33**
FortiGateが省電力モードに入った場合、正しい記述は次のうちどれですか？（2つ選択してください。）
A. FortiGateは、隔離などの重要なセキュリティ対策を引き続き実行します。
B. FortiGateが設定変更を受け付けません。
C. FortiGate はシステム全体の動作を停止し、利用可能なリソースを回復するには再起動が必要です。
D. IPSのフェイルオープングローバル設定が有効になっている場合、FortiGateはIPS検査なしでパケットを送信し続けます。
正解: (正解を表示します)
節約モードでは、FortiGateはシステムの安定性を維持するために設定変更を制限します。IPSフェイルオープンが有効になっている場合、FortiGateはリソース制約時（節約モード）でもIPS検査を行わずにトラフィックの転送を継続します。

質問: **34**
図を参照してください。FTP 用の新しいウイルス対策プロファイルを作成する際に、ウイルス対策スキャンスイッチがグレー表示されるのはなぜですか？

A. このプロファイルでは、検査対象のプロトコルはどれも有効になっていません。
B. FortiGateは、RAMが2GB未満の場合、ウイルス対策スキャン機能をサポートしません。
C. システム -> 機能の表示設定でウイルス対策スキャンが無効になっています。
D. プロファイルの機能セットはフローベースですが、プロキシベースである必要があります。
正解: (正解を表示します)
新しいウイルス対策プロファイルで検査対象プロトコル（HTTP、SMTP、POP3、IMAP、FTP、CIFS）のいずれも有効になっていないため、ウイルス対策スキャンのスイッチがグレー表示になっています。少なく

とも1つのプロトコルが有効になるまで、FortiGateはウイルス対策スキャンの有効化を許可しません。

質問: **35**
展示資料を参照してください。

この展示では、企業向けWebフィルタプロファイルのFortiGuardカテゴリベースフィルタのセクションを示しています。

管理者は、フリーウェアおよびソフトウェアダウンロードカテゴリに属するdownload.comへのアクセスをブロックする必要があります。また、同じカテゴリに属する他のウェブサイトへのアクセスは許可する必要があります。
要件を満たすための解決策を2つ挙げてください。2つ選択してください。）
A. download.com の静的 URL フィルタエントリを設定し、タイプとアクションをそれぞれワイルドカードとブロックに設定します。
B. download.com のウェブオーバーライド評価を設定し、サブカテゴリとして 悪意のあるウェブサイト」を選択します。
C. *.download.com を宛先アドレスとして、アクションが Deny で FQDN アドレス オブジェクトを持つ別のファイアウォール ポリシーを設定します。
D. フリーウェアとソフトウェアのダウンロードカテゴリのアクションを警告に設定します。
正解: **(**正解を表示します**)**
download.com をブロックするための静的 URL フィルタを作成することで、カテゴリ全体に影響を与えることなく、そのサイトだけをブロックすることが可能になります。
download.comに一致するFQDNアドレスオブジェクトに対して拒否アクションを設定した別のファイアウォールポリシーを使用することで、同じカテゴリの他のサイトを許可しつつ、download.comをブロックすることも可能です。

質問: **36**
管理者は、FortiGateデバイスをエージェントレスポーリングモードのコレクターとして動作するように設定しました。
Active Directoryのユーザーグループ情報を取得するために、管理者はFortiGateデバイスに何を追加する必要がありますか？
A. TACACSサーバー
B. LDAPサーバー
C. RADIUSサーバー
D. Keycloakサーバー
正解: **(**正解を表示します**)**
エージェントレスポーリングモードでは、FortiGateはActive Directoryに直接問い合わせてユーザーおよびグループ情報を取得します。そのためには、管理者はFortiGate上にLDAPサーバーを設定する必要があります。これにより、FortiGateはActive Directoryからユーザーグループメンバーシップの詳細を取得できるようになります。

質問: **37**
SD-WANにおけるルーティングの重要な原則を3つ挙げてください。3つ選択してください。）
A. デフォルトでは、含まれる SD-WAN メンバーが宛先への有効なルートを持たない場合、SD-WAN ルールはスキップされます。
B. SD-WANルールは、他のどのタイプのルートよりも優先されます。
C. デフォルト設定。宛先へのルートが1つしかない場合、SD-WANルールはスキップされます。
D. 通常のポリシー ルートは SD-WAN ルールよりも優先されます。
E. デフォルトでは、宛先への最適なルートがSD-WANメンバーでない場合、SD-WANルールはスキップされます。
正解: **A,B,E (**コメントを発表する**)**
SD-WANメンバーのいずれも宛先への有効なルートを持っていない場合、SD-WANルールはスキップされます。
SD-WANルールは、他のルートタイプよりも優先されます。
宛先への最適な経路がデフォルトではSD-WANメンバーでない場合、SD-WANルールはスキップされます。

質問: **38**
FortiGate管理者は、SSL VPNポータルの攻撃対象領域を縮小する必要があります。
サービス拒否（DoS）攻撃を軽減するために使用できるSSLタイマーはどれですか？
A. SSL VPN HTTPリクエストヘッダータイムアウト
B. SSL VPN dtls-hello-timeout

C. SSL VPNログインタイムアウト
D. SSL VPN アイドルタイムアウト
正解: **(**正解を表示します**)**
VPN SSL設定の構成
http-request-header-timeoutを1〜60秒に設定します。
終わり
タイマーは、部分的なHTTPリクエストによって引き起こされるSSL VPNに対するDoS攻撃を軽減するのにも役立ちます。

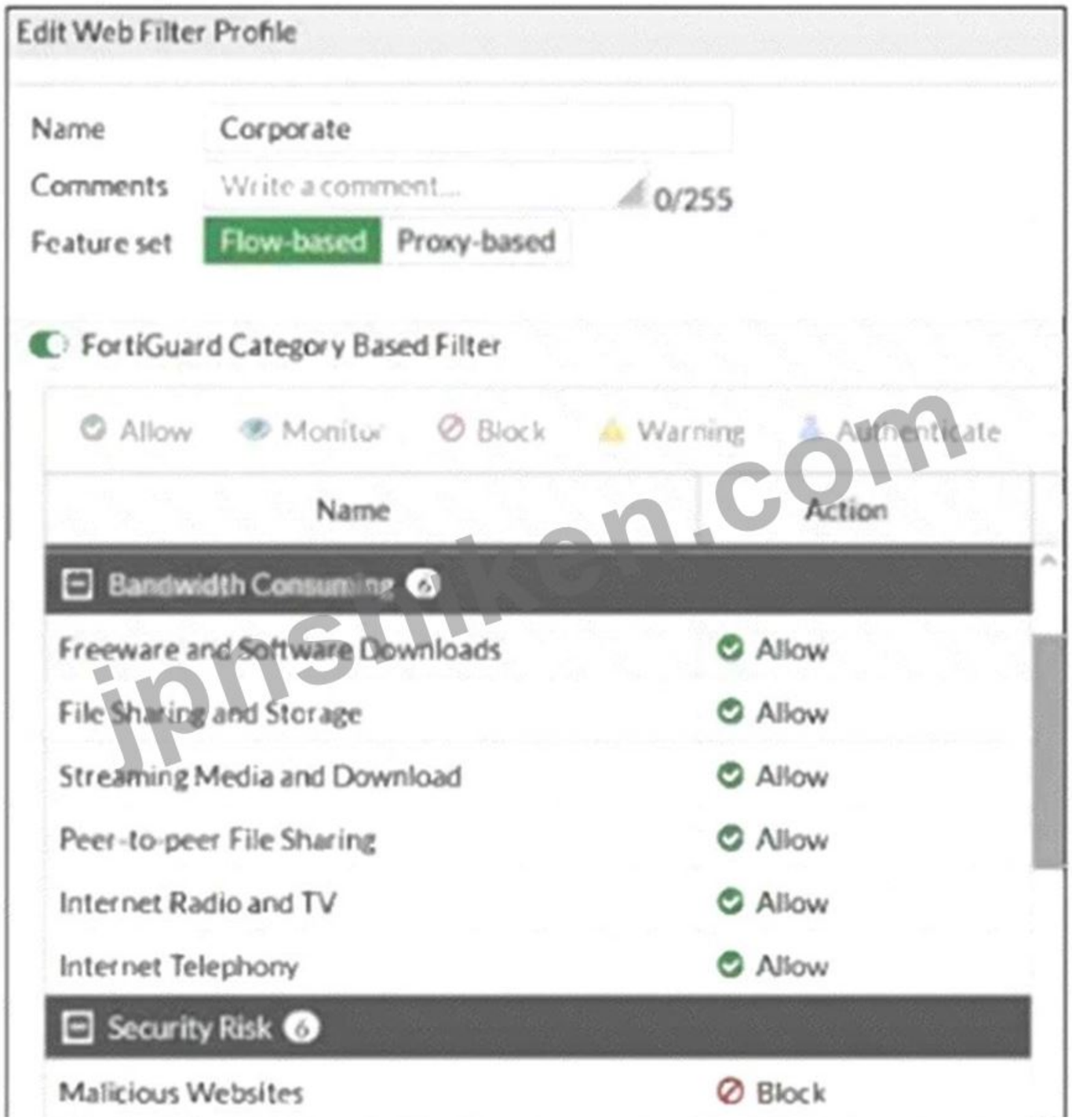
質問: **39**
HAオーバーライド設定が有効になっている場合、FortiGateの主要な選出プロセスは何ですか？
A. 接続されている監視ポート > 優先度 > HA稼働時間 > FortiGateシリアル番号
B. 監視対象ポート > 優先度 > システム稼働時間 > FortiGate シリアル番号
C. 監視対象ポート > HA稼働時間 > 優先度 > FortiGateシリアル番号
D. 監視対象ポート > システム稼働時間 > 優先度 > FortiGateシリアル番号
正解: **A (**コメントを発表する**)**
HAオーバーライドが有効になっている場合、FortiGateは次の選出順序を使用します。接続されている監視ポートの数、次にデバイスの優先度、続いてHAの稼働時間、最後にFortiGateのシリアル番号がタイブレーカーとして使用されます。

質問: **40**
展示資料を参照してください。

NOCチームは、NOC_Access管理者プロファイルを使用してFortiGateのGUIに接続します。彼らは、操作がない状態でもGUIセッションが早々に切断されないようにすることを要求しています。
管理者は、NOCチームからのこの特定の要求に応えるために、どのような設定を行う必要があるでしょうか？
A. すべてのプロファイル設定が有効になるように、NOC_Access をリストの一番上に移動します。
B. NOC_Access 管理者プロファイルの Override Idle Timeout パラメータのオフライン値を増やします。
C. すべてのNOC_Accessユーザーにスーパー管理者ロールが割り当てられていることを確認し、アクセスを保証します。
D. config system accprofile NOC_Access の下の admintimeout 値を増やします。
正解: **D (**コメントを発表する**)**
管理者アクセスプロファイルのadmintimeout設定は、GUIセッションの非アクティブタイムアウトを制御します。
この値を大きくすると、自動切断までのセッション時間が延長されます。

質問: **41**
展示資料を参照してください。

FortiGate web filter profile configuration



この展示では、企業向けWebフィルタプロファイルのFortiGuardカテゴリベースフィルタのセクションを示しています。
管理者は、フリーウェアおよびソフトウェアダウンロードカテゴリに属するdownload.comへのアクセスをブロックする必要があります。また、同じカテゴリに属する他のウェブサイトへのアクセスは許可する必要があります。
要件を満たすための解決策を2つ挙げてください。2つ選択してください。）
A. フリーウェアとソフトウェアのダウンロードカテゴリのアクションを警告に設定します。
B. download.com の Web オーバーライド評価を設定し、サブカテゴリとして悪意のある Web サイトを選択します。
C. download.com の静的 URL フィルタエントリを設定し、タイプとアクションをそれぞれワイルドカードとブロックに設定します。
D. *.download.com を宛先アドレスとして、アクションが Deny で FQDN アドレス オブジェクトを持つ別のファイアウォール ポリシーを設定します。
正解: **B,C** (コメントを発表する)

質問: **42**
図を参照してください。FortiGateデバイスがパケットをドロップした理由は何ですか？

Time	Message
Packet Trace #1 14	
06:39:29	vd-root:0 received a packet(proto=1, 10.0.11.50:3–>100.65.0.254:2048) tun_id=0.0.0.0 from port4, type=8, code=0, id=3, seq=168.
06:39:29	allocate a new session-00000ec6
06:39:29	in-[port-4], out-[]
06:39:29	len=0
06:39:29	result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000
06:39:29	find a route: flag=00000000 gw-0.0.0.0 via port2
06:39:29	in[port-4], out-[port-2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
06:39:29	gnum-100004, use addr/intf hash, len=1
06:39:29	checked gnum-100004 policy-0, ret-matched. act-accept
06:39:29	ret-matched
06:39:29	policy-0 is matched, act-drop
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	Denied by forward policy check (policy 0)

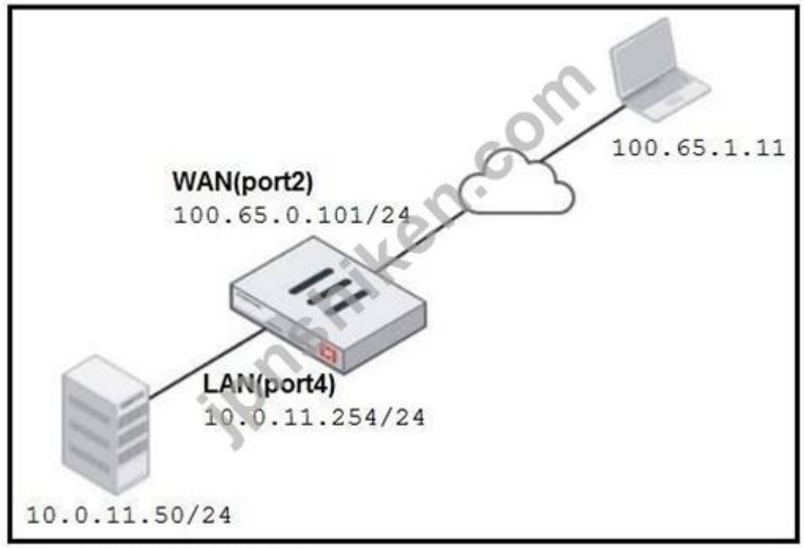
A. デフォルトの暗黙のファイアウォールポリシーと一致しました。
B. 明示的に設定されたファイアウォール ポリシーにアクション DENY で一致しました。
C. ネクストホップIPに到達できません。
D. RPFチェックに失敗しました。
正解: **(**正解を表示します**)**
パケットトレースでは、ポリシー0が一致し、act-dropおよびフォワードポリシーチェック（ポリシー）によって拒否されたことが示されています。
0) これは、パケットが明示的に設定されたファイアウォールポリシー（この場合はポリシーID 0）に一致し、そのアクションが拒否に設定されていたため、トラフィックがそれに応じて破棄されたことを意味します。

質問: **43**

展示資料を参照してください。
図に示すように、アプリケーションセンサーとそれに対応するファイアウォールポリシーを実装しました。
これらの配置から観察できる2つの要素は何ですか？ 2つ選択してください。）
A. YouTubeへのアクセスは、帯域幅超過アプリケーションおよびフィルタオーバーライド設定に基づいてブロックされています。
B. カテゴリフィルター設定に基づき、Facebookへのアクセスがブロックされています。
C. YouTube検索は、Googleアプリケーションとフィルタの上書き設定に基づいて許可されます。
D. Facebookへのアクセスは許可されていますが、動画/音声カテゴリのフィルタ設定により、Facebookの動画を再生することはできません。
正解: **(**正解を表示します**)**

質問: **44**
添付資料を参照してください。ネットワークVIPオブジェクトに接続されたFortiGateデバイスの図と、ファイアウォールポリシーの設定が示されています。
WAN（ポート2）インターフェースのIPアドレスは100.65.0.101/24です。
LAN（ポート4）インターフェースのIPアドレスは10.0.11.254/24です。
ホスト100.65.1.111がポート443でTCP SYNパケットを100.65.0.200に送信した場合、FortiGateがパケットを宛先に転送する時点で、パケットの送信元アドレス、宛先アドレス、および宛先ポートはどうなりますか？

Network diagram



VIP object configuration

A. それぞれ10.0.11.254、10.0.15.50、および4443
B. それぞれ100.65.1.111、10.0.11.50、443
C. それぞれ10.0.11.254、100.65.0.200、および443
D. それぞれ100.65.1.111、10.0.11.50、4443
正解: **(**正解を表示します**)**
VIPオブジェクトは、外部IPアドレス100.65.0.200:443を内部サーバー10.0.11.50:4443にマッピングします。
ファイアウォールポリシーでNATが無効になっているため、送信元IPアドレスは保持されます。
つまり、ホスト100.65.1.111が100.65.0.200:443に接続すると、次のようになります。
- ソースは100.65.1.111のままです。
- 宛先IPアドレスは10.0.11.50に変換されます。
- 宛先ポートは4443に変換されます。

質問: **45**
あなたは、1日のカテゴリ使用量制限を設定した「restrict_media-profile」という名前のウェブフィルタプロファイルを作成しました。
ファイアウォールポリシーにプロファイルを追加する際に、利用可能なWebプロファイルのドロップダウンリストにrestrict_media-profileが表示されません。
原因は何だろうか？
A. ファイアウォールポリシーが、詳細検査ではなく検査なしモードになっています。
B. ファイアウォール ポリシーの検査モードが、Web フィルタ プロファイルの機能セットと一致していません。
C. Webフィルタプロファイルは既に別のファイアウォールポリシーで参照されています。
D. Webフィルタプロファイルで使用されている命名規則により、ファイアウォールポリシーで制限されています。
正解: **(**正解を表示します**)**
カテゴリ使用クォータを設定したWebフィルタプロファイルでは、ファイアウォールポリシーがプロキシベース（ディープ）検査モードである必要があります。検査モードがこの要件を満たしていない場合、プロファイルはドロップダウンリストに表示されません。

質問: **46**
デバッグフローの出力を示す図を参照してください。

Debug Flow output

vd-root:0 received a packet(proto=1, 10.0.11.50:3–>100.65.0.254:2048) tun_id=0.0.0.0 from port4, type=8, code=0, id=3, seq=5.
allocate a new session-00000721
in-[port4], out-[]
len=0
result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000
find a route: flag=00000000 gw-0.0.0.0 via port2
in[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
gnum-100004, use addr/intf hash, len=3
checked gnum-100004 policy-2, ret-matched. act-accept
ret-matched
gnum-4e20, check-ffffffffa002c9c7
checked gnum-4e20 policy-6, ret-no-match, act-accept
gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
policy-2 is matched, act-drop
after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-2
Denied by forward policy check (policy 2)

デバッグフローの出力から、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. デフォルトゲートウェイはポート2に設定されています。

B. RPFチェックに失敗しました。

C. デバッグフローはUDPトラフィック用です。

D. 一致するファイアウォールポリシーにより、トラフィックが拒否されます。

正解: **A,D (**コメントを発表する**)**

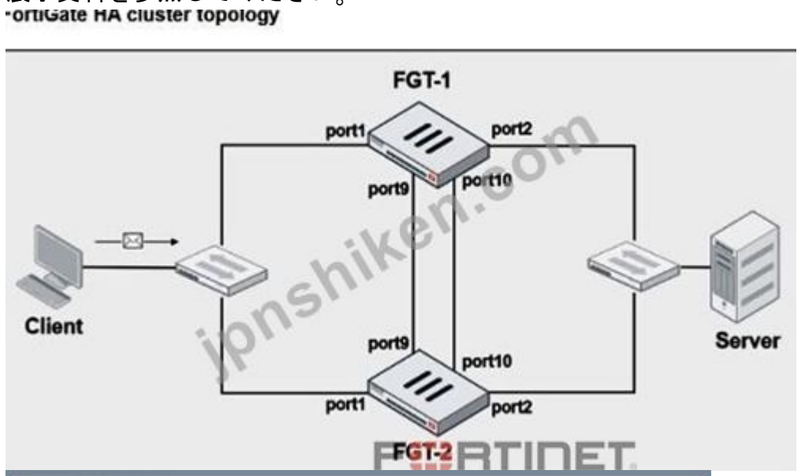
デフォルトゲートウェイはポート2に設定されています → デバッグ出力にはルートの検索が表示されます:

flag=00000000 gw-0.0.0.0 via port2 は、デフォルトルート (0.0.0.0/0) が port2 を指していることを示しています。

一致するファイアウォール ポリシーがトラフィックを拒否します → ログ行 Denied by forward policy check (policy 2)」は、ポリシー 2 が一致し、トラフィックを明示的に破棄したことを確認します。

質問: **47**

展示資料を参照してください。



New FortiGate HA configuration

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

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

FGT-1とFGT-2は、図に示すHA構成コマンドで更新されます。
HAクラスターではどのような結果が予想されるでしょうか？
A. FGT-2はオーバーライド有効化設定を持ち、FGT-1よりも優先度が高いため、プライマリとして引き継ぎます。
B. FGT-1はオーバーライド無効化設定をFGT-2と同期します。
C. HA クラスターは同期が取れなくなります。オーバーライド設定はすべての HA メンバーで一致する必要があります。
D. FGT-2の優先順位が低いため、FGT-1が引き続きプライマリになります。
正解: (正解を表示します)
HAクラスタ内のすべてのFortiGateデバイスで、オーバーライド設定は同一である必要があります。図では、FGT-1はオーバーライド無効に設定されていますが、FGT-2はオーバーライド有効に設定されています。この設定の不一致により、HAメンバーは正しく同期できず、両方のFortiGateでオーバーライド設定が一致するまでクラスタは同期が取れなくなります。

質問: **48**
図を参照してください。図に示されているルーティングテーブルに基づいて、正しい記述は次のうちどれですか？ 2つ選択してください。）

Destination	Gateway IP	Interface	Status
0.0.0.0/0	100.65.0.254	port2	Enabled
10.10.10.0/24	100.66.0.254	port3	Enabled
10.0.13.0/24	10.0.13.125	port6	Enabled

A. 厳密な RPF が無効になっている場合、送信元 IP アドレス 10.100.110.10 のパケットがポート 3 に到着することは許可されます。
B. 厳密な RPF が有効になっている場合、送信元 IP アドレス 10.100.110.10 のパケットがポート 2 に到着することは許可されます。
C. 厳密な RPF が無効になっている場合、送信元 IP アドレス 10.0.13.10 のパケットがポート 2 に到着することは許可されます。
D. 厳密な RPF が有効になっている場合、送信元 IP アドレス 10.10.10.10 のパケットがポート 2 に到着することは許可されます。
正解: (正解を表示します)
厳密な RPF が無効になっている場合、非対称ルーティングが許可されます。したがって、送信元が
10.100.110.10 (ルーティングテーブルに存在しない) でポート3に到着したパケットは、戻りルートが存在する限り (デフォルトルートはポート2経由) 受け入れられます。
厳密な RPF が無効になっている場合、ルーティング テーブルではポート 6 経由で来ることを想定しているにもかかわらず、10.0.13.10 からポート 2 に到着したパケットも許可されます。これは、厳密な RPF がない場合、システムがインターフェース チェックを強制しないためです。

質問: **49**
SSL VPN環境において、中間デバイスがトラフィックをブロックすることによって引き起こされる接続問題を分析しています。
この問題を効果的に解決できる方法は、次のうちどれですか？ 2つ選択してください。)
A. IKEフラグメンテーションを無効にすることで、大規模な証明書ネゴシエーションの問題を解決できます。
B. フラグメントドロップや大規模な証明書交換の問題を解決するには、IPsecを使用する必要があります。
C. SSL VPNトンネルモードを使用すると、ブロックされたESPおよびUDPポート 500または4500)の問題を回避できます。
D. ハブアンドスポークトポロジーをSSL VPNトンネルで構成して、ブロックされたUDPポートをバイパスできます。
正解: (正解を表示します)
このトレーニングの基本的な目的は、中間デバイスが原因で問題が発生する状況において、FortiGateのSSL VPNがIPSec VPNよりも優れている点を指摘することです。
IPsecはESPとUDP 500および4500を使用するため、これらがブロックされている場合、デフォルトでHTTPS 443)とTLS（両方ともTCP)を使用するSSL VPNトンネルモードが優れています。
UDPポートがブロックされている場合、SSL VPN トンネルモードのハブアンドスポーク)はUDPを使用しないため、優れた性能を発揮します。

質問: **50**
管理者は、NTurboをサポートするFortiGateモデルを管理します。
NTurboは、流量ベースの検査において、どのように性能を向上させるのでしょうか？
A. NTurboはファイル全体をバッファリングしてから、それをアンチウイルスエンジンに送信します。
B. NTurboは、IPSエンジンとその入力インターフェースと出力インターフェース間のトラフィックをリダイレクトするための特別なデータパスを作成します。
C. NTurboはFortiGateデバイス上で2つの検査セッションを作成します。
D. NTurboはトラフィックをコンテンツプロセッサにオフロードします。
正解: (正解を表示します)
NTurboは、IPSエンジンと入力/出力インターフェース間の高速データパスを構築することで、フローベースの検査パフォーマンスを向上させます。これにより、従来の低速なパケットパスを経由することなくトラフィックを効率的に検査できるため、CPU負荷が軽減され、フローベースのセキュリティ検査時のスループットが向上します。

質問: **51**
管理者がFortiGate上で、add-routeを有効にしたダイヤルアップIPsec VPNを設定しました。
しかし、静的ルートがルーティングテーブルに表示されません。
この状況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. 管理者はダイヤルアップインターフェースで動的ルーティングプロトコルを有効にする必要があります。
B. add-route が正しく機能するためには、管理者は静的ルートではなくポリシー ルートを使用する必要があります。
C. 管理者はフェーズ2が正常に確立されていることを確認する必要があります。

D. 管理者はフェーズ2セレクタでリモートネットワークを正しく定義する必要があります。
正解: (正解を表示します)
管理者はフェーズ 2 が正常に確立されていることを確認する必要があります → ダイヤルアップ VPN の静的ルートは、フェーズ 2 のネゴシエーションが正常に完了した後にのみ追加されます。
管理者はフェーズ 2 セレクタでリモート ネットワークを正しく定義する必要があります → ルート追加機能はフェーズ 2 セレクタに基づいてルートをインストールします。セレクタが正しくない場合、ルーティング テーブルにルートは表示されません。

質問: **52**
展示資料を参照してください。

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

このファイアウォールポリシーリストに関する記述のうち、正しいものはどれですか？
A. ファイアウォールポリシーはIDシーケンスビューで一覧表示されます。
B. ファイアウォールポリシーは、入力インターフェースと出力インターフェースのペアビューで一覧表示されます。
C. 暗黙グループには、複数の拒否ファイアウォールポリシーを含めることができます。
D. LAN to WAN、WAN to LAN、および Implicit は、シーケンス グルーピング ビュー リストです。
正解: (正解を表示します)
表示されるファイアウォールポリシー一覧は、トラフィックの方向（LANからWAN、WANからLAN、暗黙的など）に基づいてポリシーがグループ化されたシーケンスグループビューに表示されます。このビューにより、管理者は数値ID順ではなく、インターフェースのペアリングと論理的なトラフィックフローに基づいてポリシーを迅速に識別および管理できます。

質問: **53**
ネットワーク管理者がアンチウイルスを有効にし、ファイアウォールポリシーでSSL検査プロファイルを選択しました。HTTP経由でEICARテストファイルをダウンロードすると、FortiGateはウイルスを検出し、ファイルをブロックします。しかし、HTTPS経由で同じファイルをダウンロードすると、FortiGateはウイルスを検出せず、ファイルをブロックしないため、ダウンロードが許可されます。
管理者は、トラフィックが設定済みのファイアウォールポリシーに一致することを確認しました。FortiGateによるウイルス検出が失敗する理由を2つ挙げてください。（2つ選択してください。）

A. ブラウザはFortiGateの自己署名CA証明書を信頼していません。
B. EI CARテストファイルがプロトコルオプションのサイズ制限を超えています。
C. 選択された SSL 検査プロファイルでは、証明書検査が有効になっています。
D. このウェブサイトはSSL検査の対象外です。
正解: (正解を表示します)

質問: **54**
展示資料を参照してください。

HA configuration

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

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

HQ-NGFW-1 System Performance output

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

```
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes,  28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute,  0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute,  1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

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

管理者は、HAクラスタのパフォーマンスステータス出力を55秒間監視しました。
プライマリのFortiGateはどれですか？
A. パラメータ memory-failover-threshold 設定の HQ-NGFW-2
B. パラメータ優先度設定付きHQ-NGFW-2
C. パラメータ memory-failover-flip-timeout 設定の HQ-NGFW-1
D. パラメータオーバーライド設定を備えたHQ-NGFW-1
正解: **D** (コメントを発表する)
HA構成ではオーバーライドが無効になっている（set override disable）と表示されますが、それにもかかわらず、HQ-NGFW-1はより高い優先度（200）を持ち、リソース使用量と稼働時間の高さからわかるようにプライマリとして動作しています。
オーバーライド機能を使用すると、優先度の高いデバイスがプライマリデバイスとして動作を引き継ぐことができるため、HQ-NGFW-1がプライマリデバイスになります。

質問: **55**

コレクターエージェントのアドバンスモードの2つの特徴は何ですか？ 2つ選択してください。）
A. アドバンスモードでは、ネストされたグループまたは継承されたグループがサポートされます。
B. アドバンスモードでは、セキュリティプロファイルはユーザーグループにのみ適用でき、個々のユーザーには適用できません。
C. アドバンストモードでは、FortiGateをLDAPクライアントとして構成でき、FortiGate上でグループフィルタを構成できます。
D. 詳細モードでは、Windows の規則である NetBIOS: ドメイン\ユーザー名を使用します。
正解: (正解を表示します)
アドバンストモードでは、ネストされたグループや継承されたグループがサポートされ、FortiGateはActive Directory内のサブグループに属するユーザーを認識できるようになります。
アドバンストモードでは、FortiGateをLDAPクライアントとして構成し、グループフィルタを適用することで、ユーザー認証と認可をよりきめ細かく制御できます。

質問: **56**
ネットワーク管理者が、インターフェースペアビューとシーケンスビューの両方でファイアウォールポリシーを確認しています。ポリシーはそれぞれのビューで異なる順序で表示されます。
この2つの見解において、政策順序が異なるのはなぜか？
A. インターフェースペアビューのポリシーはセキュリティレベルによって優先順位が付けられますが、シーケンスビューでは管理者の手動による順序付けが厳密に適用されます。
B. シーケンスビューではルールの優先順位に基づいてポリシーをグループ化しますが、インターフェースペアビューは常にトラフィックログの順序に従います。
C. ファイアウォールは、最近のトラフィックパターンに基づいてインターフェイスペアビューのポリシーを動的に再編成しますが、シーケンスビューは静的なままです。
D. インターフェースペアビューは、一致するインターフェースに基づいてポリシーをソートし、シーケンスビューはルールの実際の処理順序を表示します。
正解: (正解を表示します)
インターフェイスペアビューでは、ポリシーが送信元インターフェイスと宛先インターフェイスごとにグループ化されて表示されますが、シーケンスビューでは、ファイアウォールによって処理される正確な順序でポリシーが表示されます。

質問: **57**
FortiGateはNATモードで動作しており、LANネットワークとDMZネットワークにそれぞれ接続された2つの物理インターフェースを備えています。
FortiGateの接続された物理インターフェースの要件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. 両方のインターフェースにインターフェースロールが割り当てられている必要があります。
B. 両方のインターフェースは、ルーティングテーブル上で直接接続されたルートを持っている必要があります。
C. 両方のインターフェースでDHCPが有効になっており、インターフェースにLANとDMZの役割が割り当てられている必要があります。
D. 両方のインターフェースにIPアドレスが割り当てられている必要があります。
正解: (正解を表示します)
インターフェースがトラフィックを正しく転送するには、ルーティングテーブルに直接接続されたルートが登録されている必要があります。
インターフェースは、それぞれのネットワーク内で通信するために、IPアドレスが割り当てられている必要があります。

質問: **58**
展示資料を参照してください。

Antivirus profile

Firewall policy

Service

- DNS
- HTTP
- HTTPS
- FTP

Firewall/Network Options

Inspection mode: Flow-based | Proxy-based

NAT

IP pool configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

Preserve source port

Protocol options: PROT default

Security Profiles

AntiVirus: AV HTTP_AV_Profile

Web filter

Video filter

DNS filter

Application control

IPS

File filter

SSL inspection: SSL certificate-inspection

FTP、HTTP、HTTPS経由でダウンロードされるファイルに対して、ウイルス対策プロファイルを実装するよう求められています。
テスト中、HTTPおよびFTPプロトコルでは正常に動作しますが、FortiGateはHTTPS経由のファイルダウンロードをブロックしません。
原因は何でしょうか？

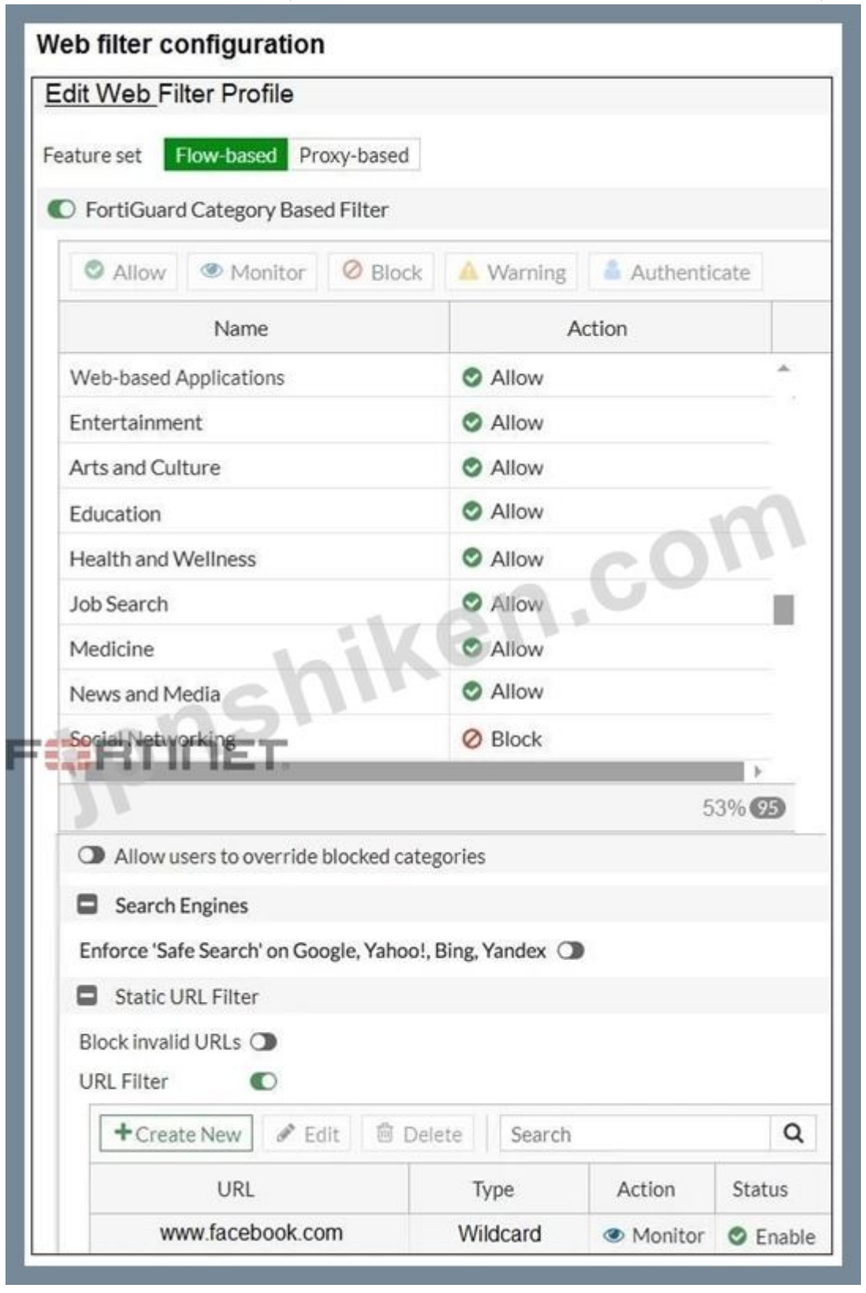
A. ウイルス対策プロファイルの機能セットがフローベースに設定されていません。
B. ファイアウォール ポリシーで Web フィルタが有効になっていないため、ウイルス対策プロファイルが補完されません。
C. ファイアウォールポリシーのアクションは拒否に設定されていません。
D. ファイアウォール ポリシーの SSL 検査モードは、ディープ コンテンツ検査ではありません。
正解: **D** (コメントを発表する)
ファイアウォールポリシーのSSL検査モードは証明書検査に設定されており、HTTPSトラフィックを復号化せずにSSL証明書のみを検査します。そのため、FortiGateはHTTPS経由でダウンロードされたファイルを検査またはブロックできません。コンテンツは暗号化されたままです。HTTPSトラフィックでウイルス対策スキャンを有効にするには、SSL検査モードをディープ検査に設定する必要があります。これにより、FortiGateはトラフィックを復号化、検査、および再暗号化できるようになります。

質問: **59**
添付の図を参照してください。この図は、リモート認証サーバーの構成の一部を示しています。

FortiGate管理者はこの設定をなぜ必要とするのですか？

A. RADIUSサーバーのシークレットを設定します。
B. FortiGateユーザーグループを認証する。
C. RADIUSサーバー上でトレーニングOUを認証し、照合します。
D. トレーニングユーザーグループのみを認証します。
正解: (正解を表示します)
Fortinet-Group-Name属性は、特定のグループに属するユーザーのみに認証を制限するために使用されます。
RADIUSサーバー上の「トレーニング」ユーザーグループ。
質問: **60**
添付資料を参照してください。管理者は、Facebookを除くすべてのソーシャルネットワーキングサイトへのアクセスをブロックするようにWebフィルタプロファイルを設定しました。しかし、ユーザーが

Facebook.comにアクセスしようとすると、FortiGuardのWebフィルタリングブロックページにリダイレクトされます。
提示された資料に基づき、管理者はFacebookへのアクセスを許可しつつ、他のすべてのソーシャルネットワーキングサイトをブロックするために、どのような設定変更を行う必要がありますか？



A. 静的URLフィルタセクションでタイプを ｢シンプル｣に変更します。

B. FortiGuard カテゴリベースフィルタでソーシャルネットワーキングのアクションを警告に設定します。

C. Webフィルタプロファイルの機能セットをプロキシベースに変更します。

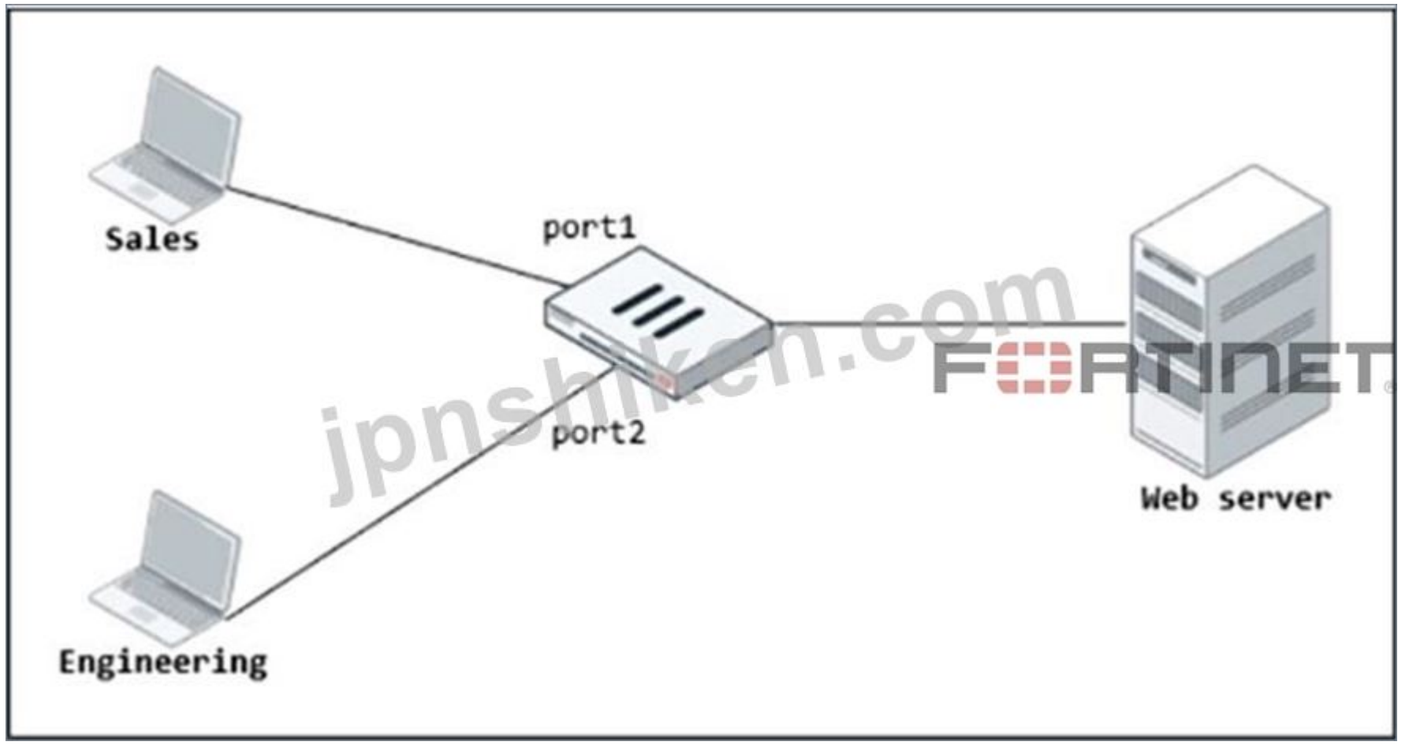
D. 静的URLフィルタで、www.facebook.comのアクションを除外に設定します。

正解: **D** (コメントを発表する)

FortiGuardのカテゴリフィルタは、Facebookを含むソーシャルネットワーキングをブロックしています。www.facebook.comの静的URLフィルタエントリは存在しますが、そのアクションは 監視｣に設定されているため、カテゴリブロックを上書きしません。他のソーシャルネットワーキングサイトをブロックしつつFacebookを許可するには、静的URLフィルタのwww.facebook.comのアクションを 除外｣に設定する必要があります。これにより、そのURLのカテゴリフィルタリングが明示的にバイパスされます。

質問: **61**

展示資料を参照してください。



FortiGateには、営業部門とエンジニアリング部門が同じセキュリティプロファイルを使用して同じWebサーバーにアクセスできるように、それぞれ独立した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、2つのポリシーを1つに統合するために、どのような操作を行う必要がありますか？
A. port1とport2を含むインターフェースグループを作成して、単一のファイアウォールポリシーを作成します。
B. 複数のインターフェース ポリシーを有効にして、同じファイアウォール ポリシーでポート 1 とポート 2 を選択します。
C. 単一のファイアウォール ポリシーで、port1 と port2 を任意のインターフェースに置き換えます。
D. 単一のファイアウォールポリシーでポート1とポート2のサブネットを選択します。
正解: **A** (コメントを発表する)
異なる受信インターフェース（port1とport2）を使用するものの、宛先、サービス、セキュリティプロファイルが同じ2つのファイアウォールポリシーを統合するには、管理者はport1とport2の両方を含むインターフェースグループを作成する必要があります。
これにより、単一のファイアウォールポリシーを両方のインターフェースからのトラフィックに適用できるため、管理が簡素化され、一貫したセキュリティ対策が維持されます。

質問: **62**
展示資料を参照してください。

この部分的な設定に基づくと、FortiGateが省電力モードに入った場合に考えられる2つの結果は何ですか？ 2つ選択してください。）

A. 管理者は設定を変更できません。

B. FortiGate は隔離アクションをスキップします。

C. 新しいセッションを許可するには、管理者は FortiGate を再起動する必要があります。

D. FortiGate は検査を必要とする新しいセッションを破棄します。

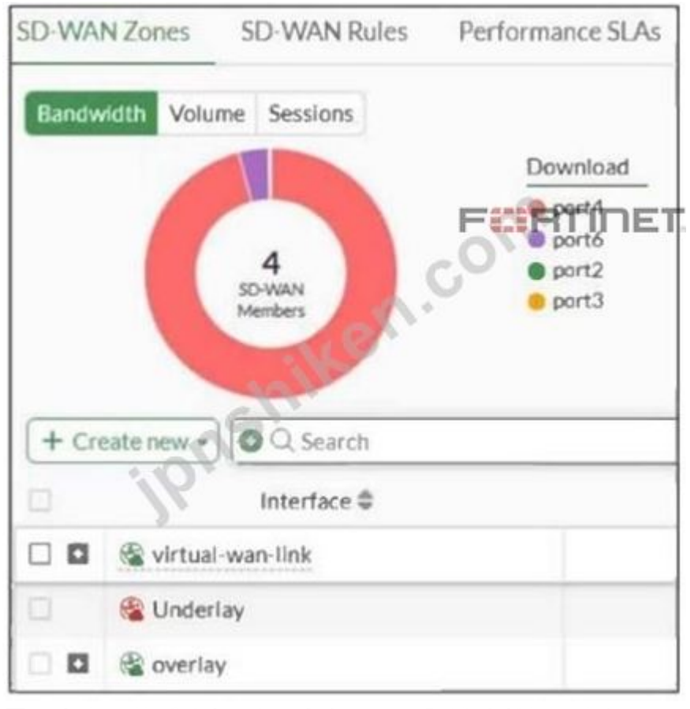
正解: **(**正解を表示します**)**

フェイルオープンモードでは、FortiGateはIPSやアンチウイルスに障害が発生した場合でもトラフィックの流れを維持するために、隔離措置をスキップします。

FortiGateは、保守モードでフェイルオープンが有効になっている場合、検査が必要な新規セッションを破棄し、潜在的に有害なトラフィックからネットワークを保護します。

質問: **63**

FortiGateのGUI上でのSD-WANゾーン構成を示す図を参照してください。



展示内容に基づくと、次のうち正しい記述はどれですか？

A. アンダーレイゾーンはデフォルトのゾーンです。

B. アンダーレイゾーンには部材がありません。

C. ポート2とポート3はゾーンに割り当てられていません。
D. 仮想WANリンクとオーバーレイゾーンを削除できます。
正解: **A** (コメントを発表する)
アンダーレイゾーンはデフォルトのSD-WANゾーンであり、通常はオーバーレイリンクや仮想リンクが追加される前のSD-WAN構成における物理インターフェースを表します。

質問: **64**
FSSOコレクターエージェントのNetAPIポーリングモードを正しく説明しているのは、次のうちどれですか？
A. NetSessionEnum 関数は、ユーザーのログアウトを追跡するために使用されます。
B. コレクターエージェントは、Windows アプリケーションイベントログを検索する必要があります。
C. コレクターエージェントは、Windows API を使用して DC にユーザーログインを照会します。
D. NetAPIポーリングは、大規模ネットワークで帯域幅の使用を増加させる可能性があります。
正解: (正解を表示します)

質問: **65**
添付資料を参照してください。管理者は、Facebookを除くすべてのソーシャルネットワーキングサイトへのアクセスをブロックするようにWebフィルタプロファイルを設定しました。しかし、ユーザーがFacebook.comにアクセスしようとすると、FortiGuardのWebフィルタリングブロックページにリダイレクトされます。
提示された資料に基づき、管理者はFacebookへのアクセスを許可しつつ、他のすべてのソーシャルネットワーキングサイトをブロックするために、どのような設定変更を行う必要がありますか？

A. www.facebook.comに対してアクションを除外設定する
静的URLフィルター内。
B. Webフィルタプロファイルの機能セットをプロキシベースに変更します。

C. FortiGuard カテゴリベースフィルタでソーシャルネットワーキングのアクションを警告に設定します。
D. 静的URLフィルタセクションでタイプをシンプルに変更します。
正解: **A (**コメントを発表する**)**

質問: **66**
展示資料を参照してください。

Time	Message
Packet Trace #1 14	
06:39:29	vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4, type=8, code=0, id=3, seq=168.
06:39:29	allocate a new session-00000ec6
06:39:29	in-[port-4], out-[]
06:39:29	len=0
06:39:29	result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000
06:39:29	find a route: flag=00000000 gw-0.0.0.0 via port2
06:39:29	in[port-4], out-[port-2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
06:39:29	gnum-100004, use addr/intf hash, len=1
06:39:29	checked gnum-100004 policy-0, ret-matched, act-accept
06:39:29	ret-matched
06:39:29	policy-0 is matched, act-drop
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	Denied by forward policy check (policy 0)

FortiGateデバイスはなぜパケットをドロップしたのですか？
A. 明示的に設定されたファイアウォール ポリシーに一致し、アクションは DENY でした。
B. RPFチェックに失敗しました。
C. デフォルトの暗黙のファイアウォールポリシーと一致しました。
D. ネクストホップIPに到達できません。
正解: **C (**コメントを発表する**)**

質問: **67**
「restrict_media-profile」という名前のWebフィルタプロファイルを作成し、カテゴリごとの日次使用量クォータを設定しました。このプロファイルをファイアウォールポリシーに追加しようとした際、利用可能なWebプロファイルのドロップダウンリストに「restrict_media-profile」が表示されません。

原因は何だろうか？
A. ファイアウォールポリシーが、詳細検査ではなく検査なしモードになっています。
B. ファイアウォール ポリシーの検査モードが、Web フィルタ プロファイルの機能セットと一致していません。
C. Webフィルタプロファイルは既に別のファイアウォールポリシーで参照されています。
D. Webフィルタプロファイルで使用されている命名規則により、ファイアウォールポリシーで制限されています。
正解: **(**正解を表示します**)**
カテゴリ使用クォータを設定したWebフィルタプロファイルでは、ファイアウォールポリシーがプロキシベース（ディープ）検査モードである必要があります。検査モードがこの要件を満たしていない場合、プロファイルはドロップダウンリストに表示されません。

質問: **68**
セキュリティファブリックの評価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. セキュリティ評価セクションのエグゼクティブサマリーを取得するにはライセンスが必要です。
B. ルートFortiGateは、セキュリティファブリック内のすべてのFortiGateデバイスの概要を提供します。
C. セキュリティ態勢カテゴリでは、PCI準拠の結果が提供されます。
D. セキュリティ評価に関するインサイトは、セキュリティ評価ページでのみ利用可能です。
正解: **A,B (**コメントを発表する**)**
セキュリティ評価セクションのエグゼクティブサマリーを取得するにはライセンスが必要です → ライセンスがない場合、セキュリティファブリックの評価に関する詳細情報は限定的にしか表示されません。
ルートFortiGateは、セキュリティファブリック内のすべてのFortiGateデバイスの情報を集約し、概要を提供することで、統合されたセキュリティ態勢の概要を示します。

質問: **69**
展示資料を参照してください。

Edit Phase 2 Selector

Name: ToBR1

Comments: Comments 0/255

Encapsulation: Tunnel Mode | Transport Mode

IP version: IPv4 | IPv6

Named address:

Local address: IP Address | Subnet Address | IP Range

10.0.11.0 255.255.255.0

Remote address: IP Address | Subnet Address | IP Range

172.20.1.0 255.255.255.0

Advanced

Encryption - authentication: AES128 - SHA1

+

Replay detection: Enable | Disable

Perfect forward secrecy (PFS): Enable | Disable

Diffie-Hellman groups:

☐ 1	☐ 2	☑ 5
☐ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

Local port: All | Specify

Edit Phase 2 Selector

Name: ToHQ

Comments: Comments 0/255

Encapsulation: Tunnel Mode | Transport Mode

IP version: IPv4 | IPv6

Named address:

Local address: IP Address | Subnet Address | IP Range

172.20.1.0 255.255.255.0

Remote address: IP Address | Subnet Address | IP Range

10.11.0.0 255.255.255.0

Advanced

Encryption - authentication: AES256 - SHA1

+

Replay detection: Enable | Disable

Perfect forward secrecy (PFS): Enable | Disable

Diffie-Hellman groups:

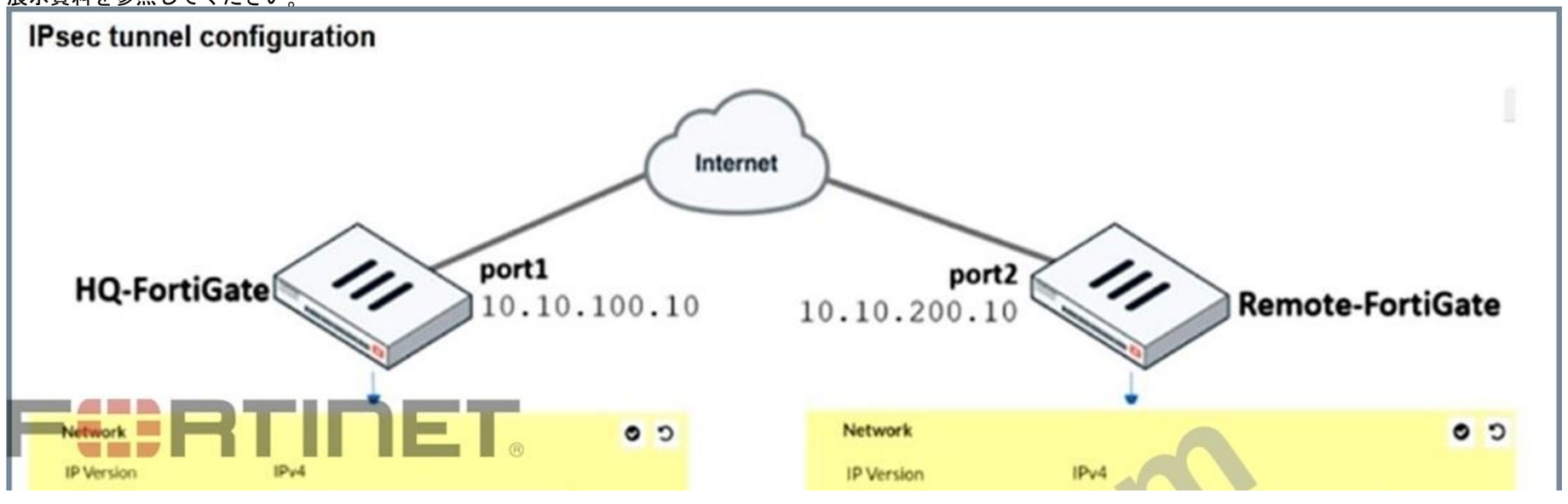
☐ 1	☐ 2	☑ 5
☑ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

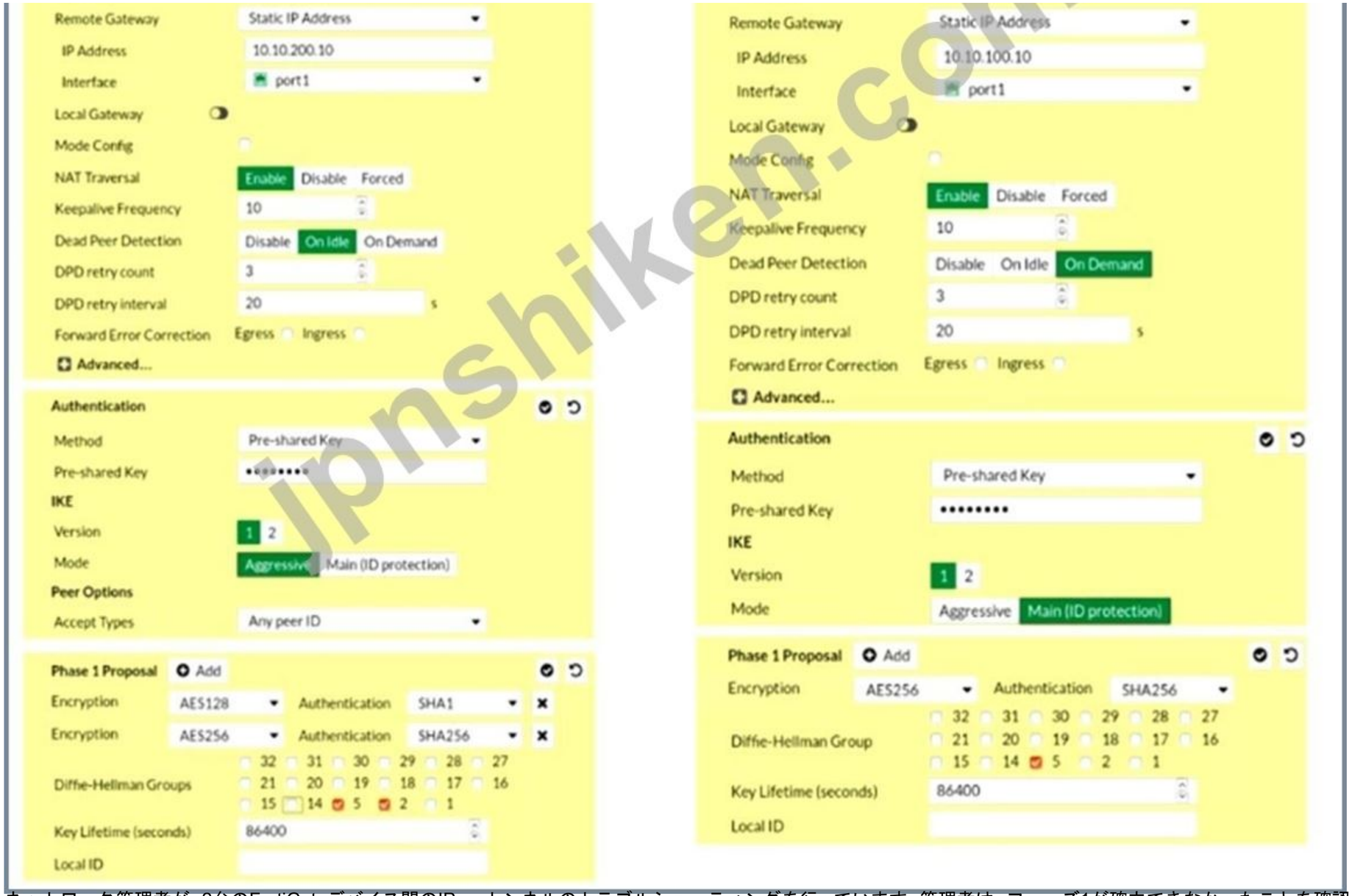
Local port: All | Specify

ネットワーク管理者が、2台のFortiGateデバイス間のIPsecトンネルのトラブルシューティングを行っています。管理者は、フェーズ1の状態は正常であることを確認しましたが、フェーズ2が起動しないことが判明しました。
図に示されているフェーズ2の構成に基づくと、フェーズ2を起動させるには、どの2つの構成変更が必要ですか？ 2つ選択してください。）

A. BR1-FGTで、秒数を43200に設定します。
B. HQ-NGFWで、Diffie-Hellmanグループ2を有効にします。
C. BR1-FGTで、リモートアドレスを10.0.11.0/255.255.255.0に設定します。
D. HQ-NGFWで暗号化をAES256に設定します。
正解: **(**正解を表示します**)**
キーの有効期間（秒は両側で一致する必要があります。BR1-FGTは14400に設定されているため、43200に設定するとHQ-NGFWと一致します。
BR1-FGTのリモートアドレスは、HQ-NGFWのローカルサブネット（10.0.11.0/24）と一致させる必要がありますが、現在は172.20.1.0/24と誤って設定されています。これを10.0.11.0/255.255.255.0に変更することで、フェーズ2セレクタが正しく動作します。

質問: **70**
展示資料を参照してください。





ネットワーク管理者が、2台のFortiGateデバイス間のIPsecトンネルのトラブルシューティングを行っています。管理者は、フェーズ1が確立できなかったことを確認しました。また、両方のFortiGateデバイスに事前共有キーを再入力し、キーが一致していることを確認しました。

フェーズ1の構成と図表に基づいて、管理者はフェーズ1を起動するためにどの2つの構成変更を行うことができますか？ 2つ選択してください。）

A. HQ-FortiGateで、IKEモードをメイン（ID保護）に設定します。

B. Remote-FortiGateで、ポート2をインターフェースとして設定します。

C. HQ-FortiGateで、Diffie-Helmanグループ2を無効にします。

D. 両方の FortiGate デバイスで、デッド ピア検出をオンデマンドに設定します。

正解: **(**正解を表示します**)**

HQ-FortiGateではIKEフェーズ1モードが「アグレッシブ」に設定されていますが、リモート-FortiGateでは「メイン（ID保護）」に設定されています。フェーズ1を確立するには、両方の側で同じIKEモードを使用する

必要があるため、HQ-FortiGateをメインモードに変更することでこの不一致を解消できます。
リモートFortiGateでは、フェーズ1のインターフェースはport1に設定されていますが、図によるとIPアドレス10.10.200.10を持つWAN側のインターフェースはport2です。IPsec設定のローカルインターフェースは物理的なWANインターフェースと一致する必要があるため、トンネルを確立するにはport2に変更する必要があります。