Fortinet.NSE7_SDW-6.4.v2024-01-17.q61

試験コード:	NSE7_SDW-6.4
試験名称:	Fortinet NSE 7 - SD-WAN 6.4
認定資格:	Fortinet
無料問題数:	61
バージョン:	v2024-01-17
アクセス数:	1089
ページビュー数:	610
https://www.jpnpdf.com/Fortinet.NSE7_SDW-6.4.v2024-01-17.q61-mondaishu.html	

最新問題: **1**
BGP タグが SD-WAN ルールでどのように機能するかを反映しているステートメントはどれですか?
A. BGP タグは、これらのルールがインストールされた順序に基づいて SD-WAN ルールと一致します。
B. BGP タグでは、すべての ADVPN インターフェイスで静的ルートの追加を有効にする必要があります。
C. ルート タグは BGP コミュニティに使用され、SD-WAN ルールには同じタグが割り当てられます。
D. SD-WAN での BGP 動的ルーティングのみを使用して VPN トポロジが形成されます
Answer: C (メーッセージを残す)
SD-WAN 6.4.5 ガイド ページ 226 ～ 227。

最新問題: **2**
添付資料を参照してください:

```
config vpn ipsec phase1-interface
    edit "FIRST VPN"
        set type dynamic
        set interface "port"
        set peertype any
        set proposal aes128-sha256 aes2
        set add-route enable
        set dhgrp 14 15 19
        set xauthtype auto
        set authusrgrp "first-group"
        set psksecret fortinet1
    next
end
```

jpnpdf.com

レスポンダの FortiGate が IPsec VPN インターフェイス上でダイナミック ルーティング プロトコルを使用している場合、正しい記述はどれですか?
A. 動的ルーティングに使用できるのは、XAuth を使用しないダイヤルアップ接続のみです。

B. ピアタイプは、一意の VPN インターフェイスに対して 1 つのピア ID のみを受け入れるように設定する必要があります
C. FortiGate が VPN 静的ルートをインストールしないようにするには、add-route を無効にする必要があります
D. 動的ルーティングの場合、フェーズ 1 タイプを静的タイプに変更する必要があります。
Answer: (解答を表示する**)**

最新問題**: 3**
展示を参照してください。
複数の IPsec VPN が 2 つのハブアンドスポーク グループ間、およびハブ 1 とハブ 2 の間のサイト間で形成されます。管理者はデュアル リージョン トポロジで ADVPN を構成しました。

トロントのユーザーがロンドンにトラフィックを送信する場合、正しい 2 つの記述はどれですか? (2つお選びください)
A. トロントはハブ 1 をバイパスするために、ハブ 2 とのサイト間トンネルを確立する必要があります。
B. トロントからロンドンへの最初のパケットは、ハブ 1 を経由してハブ 2 にルーティングされます。
C. ロンドンは、トロントのパブリック IP アドレスを含む IKE 情報メッセージを生成します。
D. トロントからロンドンへのトラフィックにより、直接サイト間 VPN の動的ネゴシエーションがトリガーされます。
Answer: B,D (メーッセージを残す**)**
SD-WAN_6.4_スタディ_ガイド 207 ページ

最新問題**: 4**
BGP タグが SD-WAN ルールでどのように機能するかを反映しているステートメントはどれですか?
A. BGP タグは、これらのルールがインストールされた順序に基づいて SD-WAN ルールと一致します。
B. ルート タグは BGP コミュニティに使用され、SD-WAN ルールには同じタグが割り当てられます。
C. SD-WAN での BGP 動的ルーティングのみを使用して VPN トポロジが形成されます
D. BGP タグでは、すべての ADVPN インターフェイスで静的ルートの追加を有効にする必要があります。
Answer: A (メーッセージを残す**)**

最新問題**: 5**
利用可能な帯域幅の割合に基づく SD-WAN トラフィック シェーピング モードを最もよく表すものは何ですか?
A. IP ごとのシェーピング モード
B. リバースポリシーシェーピングモード

C. インターフェースベースのシェーピングモード
D. 共有ポリシーシェーピングモード
Answer: C (メーッセージを残す**)**
SD-WAN 6.4.5 スタディ ガイド。124ページ

最新問題**: 6**
SD-WAN と ADVPN に関して正しいのはどれですか?
A. スポークは、静的インターフェイスとして動的 VPN をサポートします。
B. Hub FortiGate は、ADVPN を SD-WAN メンバー インターフェイスとして使用するように制限されています。
C. ダイナミック VPN は SD-Wan インターフェイスとしてサポートされていません。
D. ADVPN インターフェイスは SD-WAN インターフェイスのメンバーになることができます。
Answer: C (メーッセージを残す**)**

最新問題**: 7**
展示を参照してください。

ipnpdf.com

デバッグ出力に関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください)
A. FortiGate は、過去のトラフィック ログに基づいた統計と読み取り値を提供します。
B. トラフィック シェーパーによって制御されているトラフィックが 100 KB/s 未満です。
C. デバッグ出力には、IP ごとのシェーパー値とリアルタイムの読み取り値が表示されます。
D. このトラフィック シェーパーは、設定された制限を超えるトラフィックをドロップします。
Answer: (解答を表示する**)**

最新問題**: 8**
展示品を参照してください。

Exhibit A | Exhibit B

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

Exhibit A | Exhibit B

```
FortiGate # get router info routing-table details
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.168.73.2, port2, [1/0]
                  [1/0] via 192.168.1.1, port1, [10/0]
C       10.0.1.0/24 is directly connected, port3
C       192.168.1.0/24 is directly connected, port1
C       192.168.73.0/24 is directly connected, port2
```

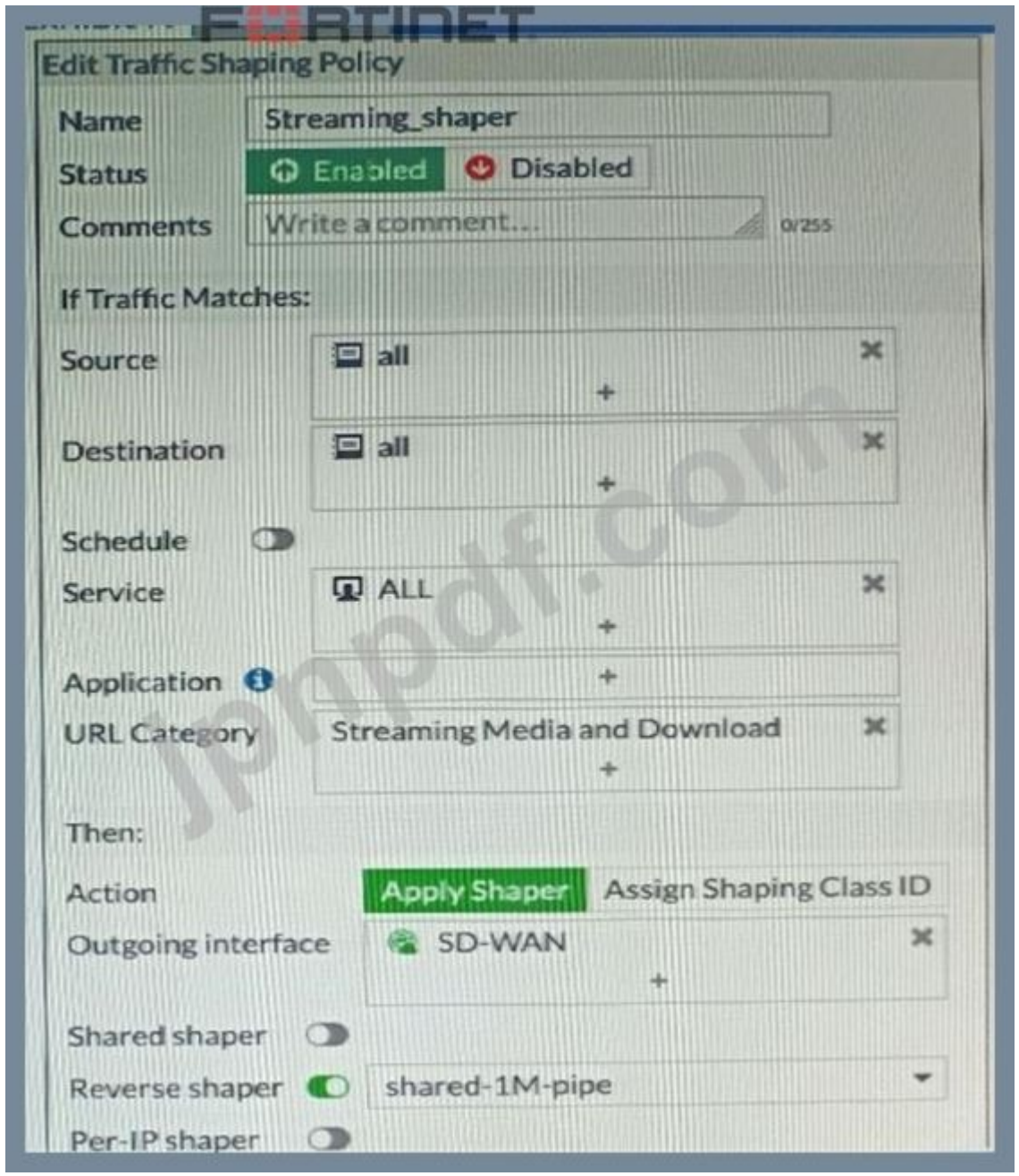
図 A はソース NAT グローバル設定を示し、図 B は FortiGate 上のルーティング テーブルを示します。
資料に基づいて、port2 インターフェイスの優先順位を 20 に増やすことに関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)

A. SNAT を使用する既存のセッションはすべてフラッシュされ、port1 経由でルーティングされます。
B. 既存のセッションはすべて、port1 と port2 の使用をブロックされます。
C. 既存のセッションはすべてポート 2 を引き続き使用し、新しいセッションはポート 1 を使用します。
D. SNAT を使用しない既存のセッションはすべてフラッシュされ、port1 経由でルーティングされます。
Answer: A,C (メーッセージを残す)

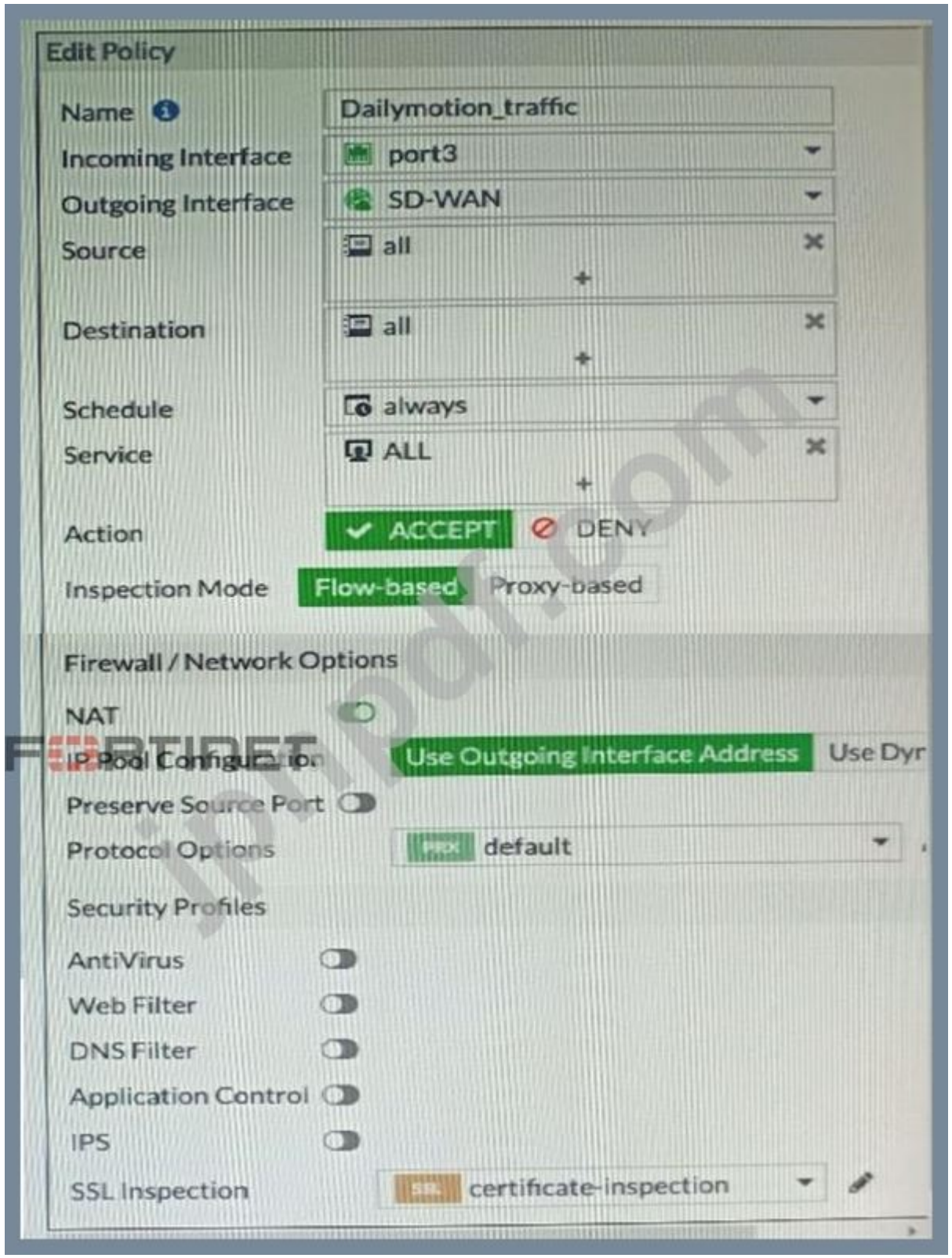
最新問題: **9**
BGP タグが SD-WAN ルールでどのように機能するかを反映しているステートメントはどれですか?
A. BGP タグは、これらのルールがインストールされた順序に基づいて SD-WAN ルールと一致します。
B. ルート タグは BGP コミュニティに使用され、SD-WAN ルールには同じタグが割り当てられます。
C. BGP タグでは、すべての ADVPN インターフェイスで静的ルートの追加を有効にする必要があります。
D. SD-WAN での BGP 動的ルーティングのみを使用して VPN トポロジが形成されます
Answer: D (メーッセージを残す)

最新問題: **10**

展示品を参照してください。
証拠品A。



証拠B。



資料 A はトラフィック シェーピング ポリシーを示し、資料 B はファイアウォール ポリシーを示しています。資料に示されているポリシーに基づいて、FortiGate が予想どおりにトラフィック シェーピングを実行していません。

FortiGate でこのトラフィック シェーピングの問題を修正するには、どのポリシーに対してどのような構成変更を行う必要がありますか?

A. シェーパー モードは、トラフィック シェーピング ポリシーの IP シェーパーごとに適用する必要があります。

B. アプリケーション制御プロファイルがファイアウォール ポリシーで有効になっている必要があります。

C. Web フィルター プロファイルがファイアウォール ポリシーで有効になっている必要があります。

D. URL カテゴリはトラフィック シェーピング ポリシーで指定する必要があります

Answer: C (メーッセージを残す)

最新問題: **11**
展示を参照してください。

VPN トンネルのステータスに関する 2 つの記述のうち、正しいものはどれですか? <2つ選択してください)

A. VPN 静的ルートは FortiGate ルーティング テーブルに追加されません。

B. FortiGate は、すべてのクライアントによって共有される単一の IPsec 仮想インターフェイスを作成しました。

C. 100.64.3.1 は、インデックス インターフェイス 1 を介して送信されるリモート IP アドレスの 1 つです。

D. ダイヤルアップ クライアントごとに個別の仮想インターフェイスがあります。

Answer: (解答を表示する)

最新問題: **12**
10 Mbps の IP ごとのトラフィック シェーパーをネットワーク全体に適用する方法を定義するステートメントはどれですか?

A. FortiGate は、各 IP アドレスに最大 10 Mbps の帯域幅を割り当てます。

B. 各 IP には最低 10 Mbps の帯域幅が保証されます

C. 割り当てられた帯域幅をユーザーの総数で割った値を 1 人のユーザーが使用します。

D. 10 Mbps の帯域幅が IP アドレス間で均等に共有されます。

Answer: A (メーッセージを残す)

参照：
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/885253/per-ip-traffic-shaper

最新問題: **13**

展示を参照してください。

パケット デバッグ フローの出力に関する結論はどれが正しいですか?

A. 元のトラフィックが送信インターフェイスの最大帯域幅を超えたため、パケットがドロップされました。

B. 元のトラフィックが送信インターフェイスの 1 秒あたりの最大パケット数を超えたため、パケットがドロップされました。

C. 元のトラフィックがトラフィック シェーパーに設定された最大帯域幅を超えたため、パケットがドロップされました。

D. 応答トラフィックがトラフィック シェーパーに設定された最大帯域幅を超えたため、パケットがドロップされました。

Answer: C (メーッセージを残す**)**

最新問題**: 14**

FortiManager を使用して FortiGate デバイスのグループのネットワークを編成および管理する 2 つの利点は何ですか? (2つお選びください)

A. すべての管理対象 FortiGate デバイスをレビューするポリシー コンプライアンス エンティティとして機能します。

B. 管理対象 FortiGate デバイスの SD-WAN パフォーマンスが向上します。

C. FortiGate に代わってプローブ信号をヘルスチェックとしてビーコンサーバーに送信します。

D. ローカル FortiGuard サーバーとして機能することで、FortiGate デバイスの WAN 使用量を削減します。

E. 管理対象 FortiGate デバイスでの SD-WAN の導入と管理を簡素化します。

Answer: D,E (メーッセージを残す**)**

最新問題**: 15**

展示を参照してください。

```
config vpn ipsec phase1-interface
    edit Hub
        set add-route enable
        set net-device disable
        set tunnel-search nexthop
    next
end

diagnose vpn tunnel list name Hub
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Hub ver=1 serial=1 100.64.1.1:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/512 options[0200]=search-
nexthop frag-rfc accept_traffic=1
proxyid_num=0 child_num=2 refcnt=20 ilast=176 olast=176 ad=/0
stat: rxp=22 txp=18 rxb=2992 txb=1752
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=2
ipv4 route tree:
100.64.3.1 1
100.64.5.1 0
172.16.1.2 1
172.16.1.3 0
```

VPN トンネルのステータスに関する 2 つの記述のうち、正しいものはどれですか? <2つ選択してください)

A. ダイヤルアップ クライアントごとに個別の仮想インターフェイスがあります。

B. VPN 静的ルートは FortiGate ルーティング テーブルに追加されません。

C. FortiGate は、すべてのクライアントによって共有される単一の IPsec 仮想インターフェイスを作成しました。

D. 100.64.3.1 は、インデックス インターフェイス 1 を介して送信されるリモート IP アドレスの 1 つです。

Answer: C,D (メーッセージを残す)

net-device が無効になっている場合、FortiGate は、同じダイヤルアップ VPN に接続しているすべての IPSEC クライアントによって共有される単一の IPSEC 仮想インターフェイスを作成します。この場合、トンネル検索設定によって、FortiGate が各リモート クライアントの背後にあるネットワークを学習する方法が決まります。

最新問題**: 16**

SD-WAN でスポーク間の IPsec VPN 動的ショートカット トンネルとハブへの静的トンネルを組み合わせることができる機能はどれですか?

A. OCVPN

B. グレー

C. ADVPN

D. SSLVPN

Answer: C (メーッセージを残す)

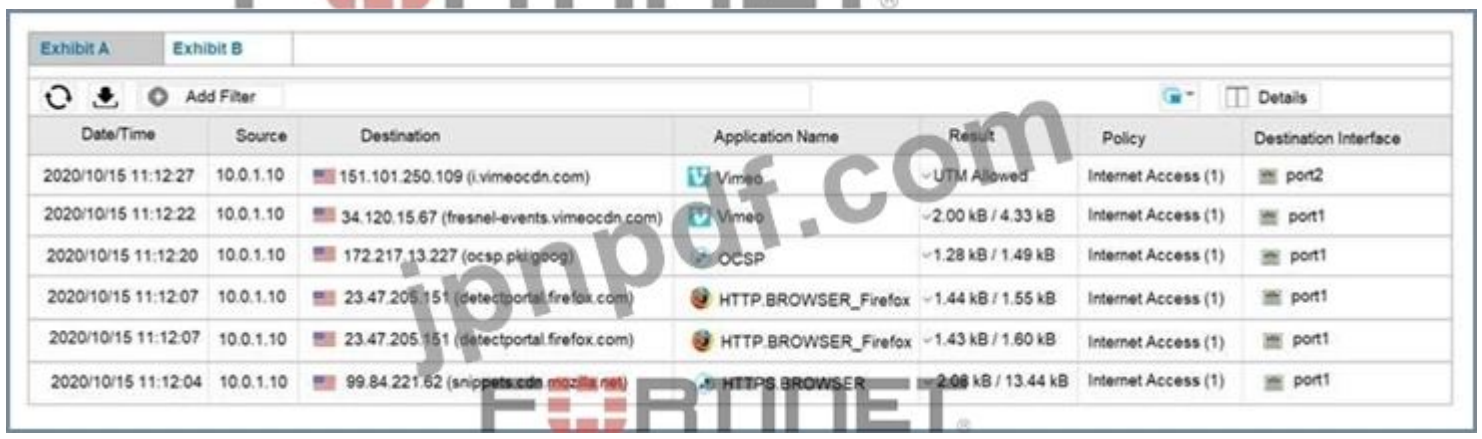
有効な **NSE7_SDW-6.4** 問題集は GoShiken.com が提供された合格しやすい NSE7_SDW-6.4 試験問題集！ GoShiken.com が最新の **NSE7_SDW-6.4** 試験問題集を提供しています。GoShiken.com NSE7_SDW-6.4 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SDW-6.4 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE7_SDW-6.4-mondaishu.html (**8230%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **17**

展示品を参照してください。

Exhibit A | Exhibit B

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Google.ICMP	all	Google-ICMP	Latency	port1, port2
2	Vimeo	all	Vimeo		port2
3	All_Access_Rules	all	all		port1
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any



資料 A は SD-WAN ルールを示し、資料 B はトラフィック ログを示します。SD-WAN トラフィック ログには、FortiGate がトラフィックを処理した方法が反映されます。

構成された SD-WAN ルールがトラフィックを処理する方法に関する 2 つの記述はどれが真実ですか? (2つお選びください。)

A. SD-WAN ルールは、ファイアウォール ポリシーと同じ方法で上から下に評価されます。

B. All_Access_Rules ルールは、SD-WAN メンバー インターフェイス間で Vimeo アプリケーション トラフィックの負荷を分散します。

C. アプリケーションの最初のセッションでは、正しいルールを適用するために学習フェーズが行われます。

D. パラメーターはソースと宛先を幅広くカバーするため、暗黙的なルールは他のすべてのルールをオーバーライドします。

Answer: A,C (メーッセージを残す)

最新問題: **18**
FortiGate は、10 Mbps の IP ごとのトラフィック シェーパーの対象となるトラフィックに対してどのアクションを実行しますか?
A. FortiGate は、すべての送信元 IP アドレス間で 10 Mbps の帯域幅を均等に共有します。
B. FortiGate は、トラフィック シェーピングを元のトラフィック方向にのみ適用します。
C. FortiGate は、各送信元 IP アドレスを最大帯域幅 10 Mbps に制限します。
D. FortiGate は、各送信元 IP アドレスに対して最低 10 Mbps の帯域幅を保証します。
Answer: (解答を表示する)

最新問題: **19**
展示を参照してください。

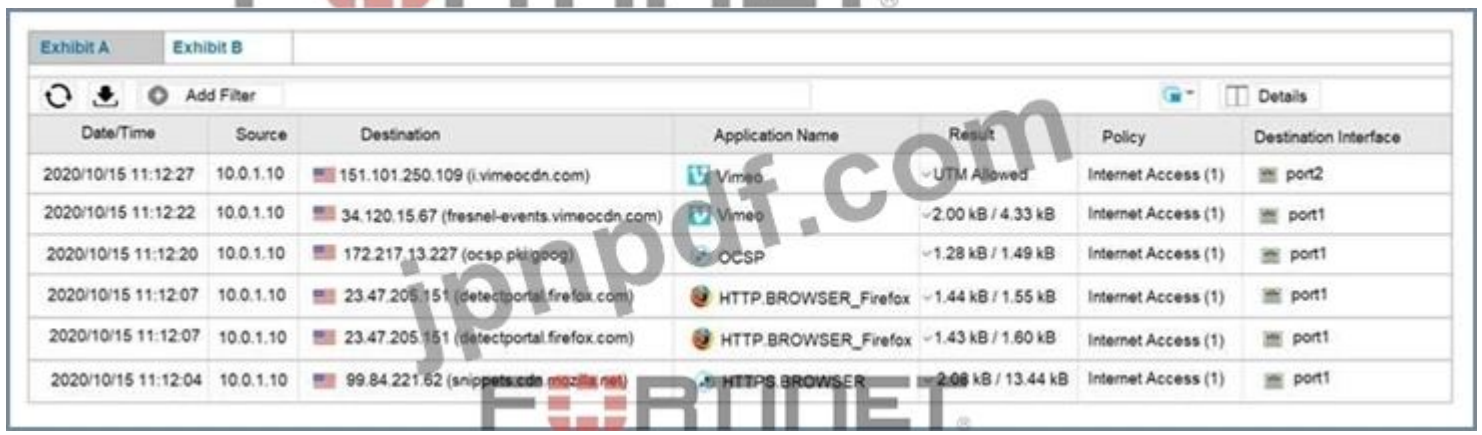
```
config vpn ipsec phase1-interface
    edit Hub
        set add-route enable
        set net-device disable
        set tunnel-search nexthop
    next
end

diagnose vpn tunnel list name Hub
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Hub ver=1 serial=1 100.64.1.1:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/512 options[0200]=search-
nexthop frag-rfc accept_traffic=1
proxyid_num=0 child_num=2 refcnt=20 ilast=176 olast=176 ad=/0
stat: rxp=22 txp=18 rxb=2992 txb=1752
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=2
ipv4 route tree:
100.64.3.1 1
100.64.5.1 0
172.16.1.2 1
172.16.1.3 0
```

VPN トンネルのステータスに関する 2 つの記述のうち、正しいものはどれですか? <2つ選択してください)
A. 100.64.3.1 は、インデックス インターレース 1 を介して送信されるリモート IP アドレスの 1 つです。
B. VPN 静的ルートが FortiGate ルーティング テーブルに入力されないようにします。
C. ダイヤルアップ クライアントごとに個別の仮想インターフェイスがあります。
D. FortiGate は、すべてのクライアントによって共有される単一の IPsec 仮想インターフェイスを作成しました
Answer: C (メーッセージを残す)

最新問題: **20**
展示品を参照してください。

Exhibit A | Exhibit B

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Google.ICMP	all	Google-ICMP	Latency	port1, port2
2	Vimeo	all	Vimeo		port2
3	All_Access_Rules	all	all		port1
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any



資料 A は SD-WAN ルールを示し、資料 B はトラフィック ログを示します。SD-WAN トラフィック ログには、FortiGate がトラフィックを処理した方法が反映されます。

構成された SD-WAN ルールがトラフィックを処理する方法に関する 2 つの記述はどれが真実ですか? (2つお選びください。)

A. アプリケーションの最初のセッションでは、正しいルールを適用するために学習フェーズが行われます。

B. SD-WAN ルールは、ファイアウォール ポリシーと同じ方法で上から下に評価されます。

C. All_Access_Rules ルールは、SD-WAN メンバー インターフェイス間で Vimeo アプリケーション トラフィックの負荷を分散します。

D. パラメーターはソースと宛先を幅広くカバーするため、暗黙的なルールは他のすべてのルールをオーバーライドします。

Answer: (解答を表示する**)**

最新問題**: 21**

展示を参照してください。

SD-WAN ルールのコマンド ルートタグに関する記述のうち、正しいものはどれですか?

A. SD-WAN ルールでロード バランシングを行い、ルート タグを使用してトラフィックを割り当てることができます。

B. 各ルートにタグを付け、ルーティング テーブル内のタグを参照します。

C. BGP コミュニティのルート タグを使用し、同じタグを持つ SD-WAN ルールを割り当てます。

D. ルールの順序に基づいて、ルート タグが SD-WAN ルールと一致することを確認します。

Answer: C (メーッセージを残す)

SD-WAN 6.4.5 ガイド ページ 226。

最新問題**: 22**

集中 VPN 管理の使用に関する 2 つのタスクのうち、正しいものはどれですか? (2つお選びください。)

A. フルメッシュ、スター、ダイヤルアップ VPN トポロジを構成できます。

B. SD-WAN 展開では VPN ゾーンを有効にする必要があります。

C. VPN コミュニティを構成して、すべての VPN ゲートウェイで共有される共通の IPsec 設定を定義します。

D. FortiManager は、管理対象ゲートウェイと外部ゲートウェイの両方に VPN 設定をインストールします。

Answer: A,C (メーッセージを残す)

最新問題**: 23**

展示品を参照してください。

証拠品A。

証拠B。

資料 A は SD-WAN ルールを示し、資料 B はトラフィック ログを示します。SD-WAN トラフィック ログには、FortiGate がトラフィックを処理した方法が反映されます。
構成された SD-WAN ルールがトラフィックを処理する方法に関する 2 つの記述はどれが真実ですか? (2つお選びください。)
A. SD-WAN ルールは、ファイアウォール ポリシーと同じ方法で上から下に評価されます。
B. パラメーターはソースと宛先を幅広くカバーするため、暗黙的なルールは他のすべてのルールをオーバーライドします。
C. All_Access_Rules ルールは、SD-WAN メンバー インターフェイス間で Vimeo アプリケーション トラフィックの負荷を分散します。
D. アプリケーションの最初のセッションは、正しいルールを適用するために学習フェーズを通過します。
Answer: (解答を表示する**)**

最新問題**: 24**
ハブまたはスポーク FortiGate で ADVPN のリアルタイム トラブルシューティングを実行するには、どの CLI コマンドを使用しますか?
A. ipsecトンネルリストの取得
B. デバッグアプリケーション ike を診断します。
C. ルーター情報の取得 ルーティングテーブル
D. sys virtual-wan-link サービスを診断します。
Answer: (解答を表示する**)**

最新問題**: 25**
SD-WAN ルールの構成に使用できる 3 つのパラメータはどれですか? (3つお選びください。)
A. アプリケーションの署名
B. 物理リンク接続の種類
C. URL カテゴリ
D. 送信元および宛先の IP アドレス
E. インターネット サービス データベース (ISDB) アドレス オブジェクト
Answer: (解答を表示する**)**
SD-WAN 6.4.5 ガイド 76 ページ。

最新問題**: 26**
SD-WAN と ADVPN に関して正しいのはどれですか?
A. ADVPN インターフェイスは SD-WAN インターフェイスのメンバーになることができます。
B. Hub FortiGate は、ADVPN を SD-WAN メンバー インターフェイスとして使用するように制限されています。
C. スポークは、静的インターフェイスとして動的 VPN をサポートします。
D. ダイナミック VPN は SD-Wan インターフェイスとしてサポートされていません。
Answer: A (メーッセージを残す**)**

最新問題: **27**
SD-WAN ルールのインターフェイス情報と状態を表示するには、どの診断コマンドを使用できますか?
A. sys sdwan ルートタグリストを診断します。
B. sys sdwan サービスを診断します。
C. sys sdwan メンバーを診断します。
D. sys sdwan ネイバーを診断します。
Answer: B (メーッセージを残す**)**
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Diagnostic-commands-to-check-the-status-of-the-SD/ta-p/194246

最新問題: **28**
SD-WAN オーケストレーターが FortiManager と連携するときに果たす 2 つの役割は何ですか? (2つお選びください)
A. FortiManager 上の管理拡張機能の一部として実行するために、Fortinet によってリリースおよび署名されたアプリケーションとして機能します。
B. スタンドアロン デバイスとして機能し、FortiManager による管理対象 FortiGate デバイス上の SD-WAN インターフェイスの管理を支援します。
C. SD-WAN インターフェイスが有効になっているハブ FortiGate として機能し、他の FortiGate デバイスとともに FortiManager によって管理されます。
D. FortiManager によって管理される FortiGate デバイス上の SD-WAN ネットワークを構成および監視します。
Answer: (解答を表示する**)**

最新問題: **29**
過去 10 分間のインターフェイス固有の SLA ログを表示するには、どの診断コマンドを使用できますか?
A. sys virtual-wan-link ヘルスチェックを診断します。
B. sys virtual-wan-link ログを診断します。
C. sys virtual-wan-link sla-log を診断します。
D. sys virtual-wan-link intf-sla-log を診断します。
Answer: C (メーッセージを残す**)**
参照：
https://community.fortinet.com/t5/FortiGate/Technical-Tip-SLA-Logging/ta-p/190934

最新問題: **30**
展示品を参照してください。

Exhibit A | Exhibit B

Edit Policy

Name: Internet Access

Incoming interface: port3

Outgoing interface: virtual-wan link

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT | DENY

Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options

NAT: enabled

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic

Preserve Source Port: disabled

Protocol Options: PROT default

FORTINET
iprnpdf.com

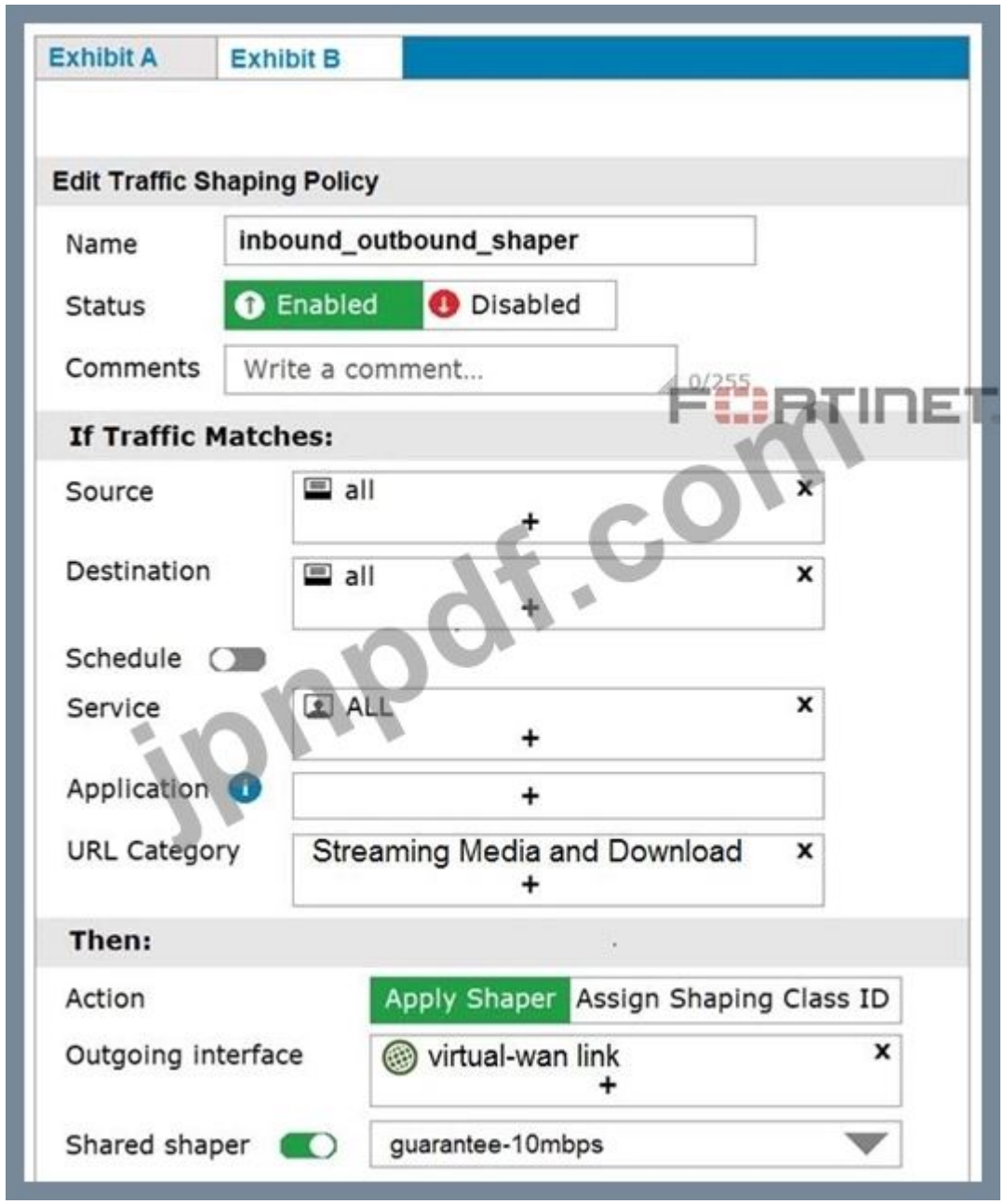


図 A はファイアウォール ポリシーを示し、図 B はトラフィック シェーピング ポリシーを示します。
トラフィック シェーピング ポリシーは、すべての送信トラフィックに適用されます。ただし、受信トラフィックはシェーピング ポリシーによって評価されません。
展示内容に基づいて、トラフィック シェーピングを受信トラフィックに適用できるようにするには、どのポリシーでどのような設定変更を行う必要がありますか?

A. トラフィック シェーピング ポリシーで、[アクション] として [シェーピング クラス ID の割り当て] を選択します。
B. トラフィック シェーピング ポリシーで、リバース シェーパーを有効にし、使用するトラフィック シェーパーを選択します。
C. 新しいファイアウォール ポリシーを作成し、SD-WAN ゾーンを受信インターフェイスとして選択します。
D. ファイアウォール ポリシーで、検査モードとしてプロキシベースを選択します。
Answer: (解答を表示する**)**

最新問題: **31**
展示品を参照してください。

jpnpdf.com

Exhibit A | Exhibit B

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
DC_PBX_SLA	4.2.2.2	port1: 0.00%	port1: 32.80ms	port1: 8.58ms	5	5
	4.2.2.1	port2: 0.00%	port2: 55.36ms	port2: 8.37ms		

Exhibit A | Exhibit B

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(dead), packet-loss(75.000%) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(50.477), jitter(3.699)
sla_map=0x1

NGFW -1 # diagnose sys virtual-wan-link service

Service(1): Address Mode(IPV4) flags=0x0
  Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(DC_PBX_SLA)
  Members:
    1: Seq_num(2 port2), alive, latency: 50.233, selected
    2: Seq_num(1 port1), dead
  Internet Service: Microsoft-Skype_Teams(327781,0,0,0)
  Src address:
      0.0.0.0-255.255.255.255
```

図 A はパフォーマンス SLA を示し、図 B は SD-WAN 診断出力を示します。
展示物に基づいて、どの記述が正しいでしょうか?
A. SD-WAN メンバー インターフェイスは、非アクティブなインターフェイスの SLA 状態の影響を受けます。
B. 両方の SD-WAN メンバー インターフェイスで個別の SLA ターゲットが使用されています。
C. ポート 1 は、ポート 1 の出力を通じてトラフィックがオフロードされなかったため、デッド状態になりました。
D. SLA サーバーからの要求が 5 回応答されなかった後、ポート 1 の SLA 状態はデッド状態になります。
Answer: (解答を表示する**)**

有効な **NSE7_SDW-6.4** 問題集は GoShiken.com が提供された合格しやすい NSE7_SDW-6.4 試験問題集！ GoShiken.com が最新の **NSE7_SDW-6.4** 試験問題集を提供しています。GoShiken.com NSE7_SDW-6.4 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SDW-6.4 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE7_SDW-6.4-mondaishu.html (**8230%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **32**
SD-WAN ルールのインターフェイス情報と状態を表示するには、どの診断コマンドを使用できますか?
A. sys virtual-wan-link サービスを診断します。
B. sys virtual-wan-link ルートタグリストを診断します。

C. sys virtual-wan-link メンバーを診断します。
D. sys virtual-wan-link ネイバーを診断します。
Answer: D (メーッセージを残す)

最新問題**: 33**
SD-WAN 論理インターフェイスが有効になった後に送信インターフェイスを選択するための 2 つの最小構成要件は何ですか? (2つお選びください)
A. SD-WAN ルールで受信インターフェイスを指定します。
B. 送信インターフェースのルーティングコストを指定します。
C. SD-WAN 分散戦略を選択します。
D. SD-WAN ルールのインターフェイス設定を構成します。
Answer: D (メーッセージを残す)

最新問題**: 34**
lnkmtd プロセスは何を担当しますか?
A. ルートタグアドレスのフラッシュ
B. インターフェース品質情報のロギング
C. 処理パフォーマンス SLA プローブ
D. リンクの帯域幅の飽和を監視します。
Answer: D (メーッセージを残す)

最新問題**: 35**
lnkmtd プロセスは何を担当しますか?
A. リンクの帯域幅の飽和を監視します。
B. 処理性能 SLA プローブ
C. ルートタグアドレスのフラッシュ
D. インターフェース品質情報のロギング
Answer: (解答を表示する)
SD-WAN 6.4.5 ガイド ページ 105。

最新問題**: 36**
SD-WAN での BGP ルートの使用について正しいのはどれですか?
A. 外部 BGP を使用する必要があります。
B. AS パスの先頭を設定する必要があります。
C. 学習されたルートは、SD-WAN ルールの動的宛先として使用できます。
D. オーバーレイ リンクとアンダーレイ リンクの両方のトラフィックをルーティングするには、BGP を使用する必要があります。
Answer: C (メーッセージを残す)

最新問題**: 37**

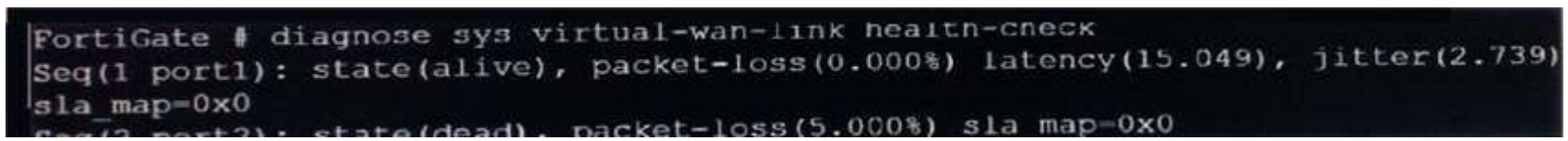
IKE ネゴシエーションを実行する際の IPsec フェーズ 1 メイン モードとアグレッシブ モードの違いを説明している 2 つのステートメントはどれですか? (2つお選びください)
A. イニシエーターとレスポンダーの間で 3 つのパケットではなく、合計 6 つのパケットが交換されます。
B. Diffie Hellman キーの使用は応答者によって制限されており、開始者の承認が必要です
C. ピア ID は、提案されたセキュリティ ポリシーとともに、イニシエータからの最初のパケットに含まれます。
D. XAuth は、ユーザー名とパスワードを必要とする追加の認証レベルとして有効になっています。
Answer: (解答を表示する**)**

最新問題**: 38**
アプリケーション制御を構成するときに SD WAN ルールを使用することが効果的であるのはなぜですか?
A. アプリケーションの種類に基づいてトラフィックの負荷分散ができるため
B. SD-WAIM ルールはファイアウォール ポリシーから独立しているため、アプリケーションの制御を回避できます。
C. アプリケーション データベースは管理者によって手動で保守されるため
D. ファイアウォール ポリシーで証明書の完全な検査を使用する必要があるため
Answer: A (メーッセージを残す**)**

最新問題**: 39**
過去 10 分間のインターフェイス固有の SLA ログを表示するには、どの診断コマンドを使用できますか?
A. sys sdwan ログを診断します。
B. sys sdwan ヘルスチェックを診断します。
C. sys sdwan intf-sla-log を診断します。
D. sys sdwan sla-log を診断します。
Answer: D (メーッセージを残す**)**
sys sdwan intf-sla-log を診断します -> 帯域幅の使用率のみを表示します
sys sdwan sla-log を診断 -> パケット損失、遅延、ジッター、MOS を表示

最新問題**: 40**
展示品を参照してください。
証拠品A。

証拠B。



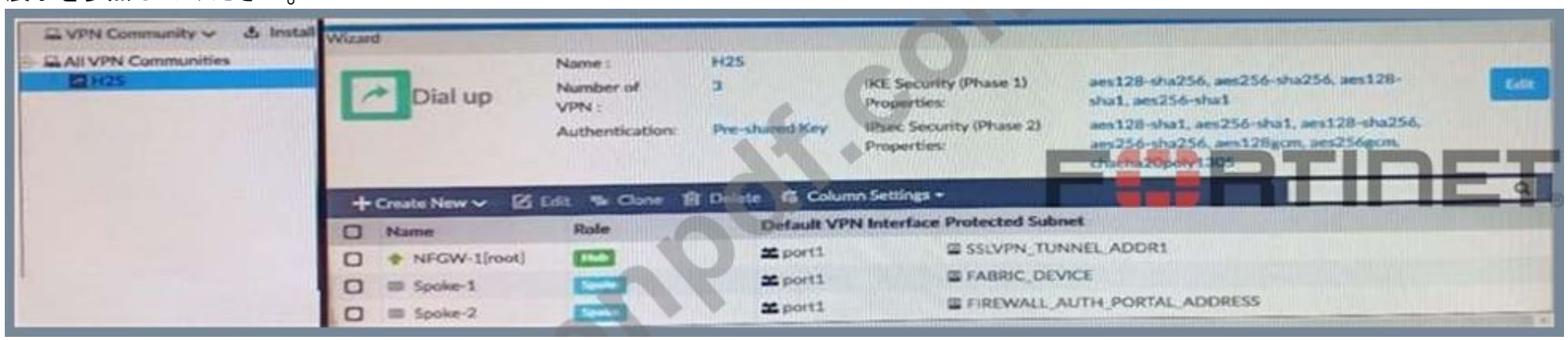
資料 A は SD-WAN パフォーマンス SLA を示し、資料 B は参加している SD-WAN メンバーの健全性を示しています。
展示物に基づいて、どの記述が正しいでしょうか?

A. ポート 2 はステータスがアライブからデッドに変わるまで 500 ミリ秒待つ必要があります。
B. デッド メンバー インターフェイスは、管理者が手動でインターフェイスを戻すまで使用できません。
C. チェック間隔は、メンバー インターフェイスによって送信されたパケットが失われたとみなされるまでの待機時間です。
D. ポート 2 の SLA 状態が、SLA サーバーからの未応答リクエストが連続 3 件を超えました。
Answer: D (メーッセージを残す**)**

最新問題**: 41**
FortiAnalyzer の事前定義テンプレートの目的は何ですか?

A. 必要に応じて編集および変更できます。
B. 事前定義されたテキスト、グラフ、マクロを含むレポート レイアウトを指定します。
C. 期間、デバイスの選択、スケジュールを含むレポート設定を指定します。
D. 模擬レポートを生成するための事前定義されたデータが含まれています
Answer: (解答を表示する**)**
FortiAnalyzer 6.4 スタディ ガイド 197 ページ

最新問題**: 42**
展示を参照してください。



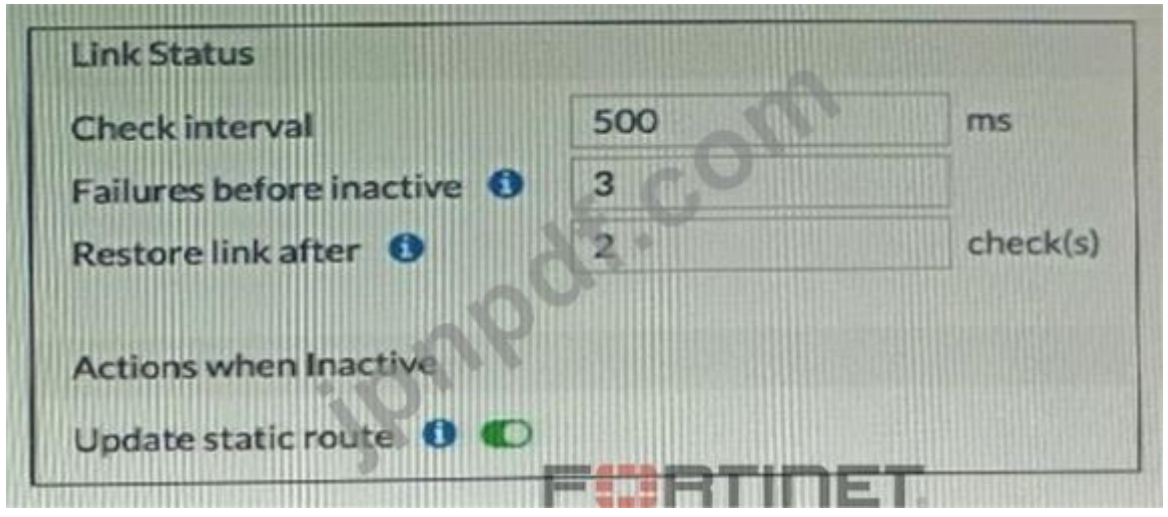
ADVPN を有効にするには何を設定する必要がありますか?

A. 各 VPN デバイスには、フェーズ 1 で個別に構成された一意の事前共有キーがあります。
B. ハブ VPN では、デバイスのみが追加のフェーズ 1 セットを必要とします。
C. 保護されたサブネットは、オブジェクトをすべて (0.0 .0. o/o) にアドレス指定するように設定する必要があります。
D. ADVPN は、管理対象外の FortiGate デバイスでのみ有効にする必要があります。
Answer: A (メーッセージを残す**)**

最新問題**: 43**
従来の VPN トポロジに代わる ADVPN ソリューションの実装の利点を反映している 2 つの記述はどれですか? (2つお選びください)

A. スポークツースポークのトラフィックがハブを介してトンネルを通過する必要がなくなりました。
B. スポーク間にオンデマンド トンネルを作成することで、すべてのサイト間に直接接続を提供します。
C. 物理的な距離に基づいて、ハブとスポーク間のコストと重量を動的に割り当てます。
D. プライマリ リンクで障害が発生した場合に備えて、ハブアンドスポーク間に冗長トンネルを作成します。
Answer: A,D (メーッセージを残す**)**

最新問題**: 44**
展示品を参照してください。
証拠品A。



証拠B。

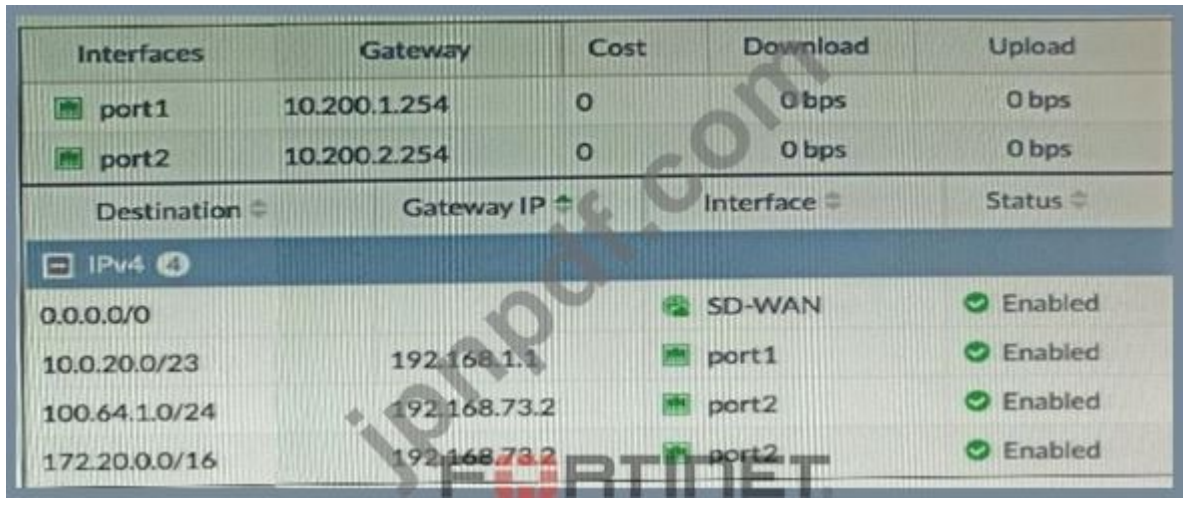


図 A は SD-WAN パフォーマンス SLA を示し、図 B は SO-WAN インターフェイスとスタティック ルート構成を示します。
ポート 1 とポート 2 は SD-WAN のメンバー インターフェイスであり、ポート 2 は障害しきい値に達するとデッド メンバーになります。
デッド メンバーに関する記述はどれが正しいですか?
A. サブネット 100 .64.1.0/23 および 172 。２０0.0/16 はポート 1 経由でのみ到達可能
B. 死亡したメンバーを生き返らせるには手動の管理者アクセスが必要です
C. SD-WAN インターフェイスが無効になり、ポート 1 が WAN インターフェイスになります。
D. SLA サーバーから 1 つの応答を受信すると、ポート 2 がアクティブになる可能性があります
Answer: A (メーッセージを残す**)**

最新問題: **45**
過去 10 分間のインターフェイス固有の SLA ログを表示するには、どの診断コマンドを使用できますか?
A. sys virtual-wan-link ヘルスチェックを診断します。
B. sys virtual-wan-link ログを診断します。
C. sys virtual-wan-link sla-log を診断します。
D. sys virtual-wan-link intf-sla-log を診断します。
Answer: C (メーッセージを残す**)**
説明/参照: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/943037/sla-logging

最新問題: **46**
展示を参照してください。

デバッグ出力に関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください)
A. トラフィックシェーパーによって制御されているトラフィックが 1 Kbps 未満
B. FortiGate は、過去のトラフィック ログに基づいて統計と測定値を提供します。
C. デバッグ出力には、IP ごとのシェーパー値とリアルタイムの読み取り値が表示されます。
D. このトラフィック シェーパーは、設定された制限を超えるトラフィックをドロップします。
Answer: B,C (メーッセージを残す**)**

有効な **NSE7_SDW-6.4** 問題集は GoShiken.com が提供された合格しやすい NSE7_SDW-6.4 試験問題集！ GoShiken.com が最新の **NSE7_SDW-6.4** 試験問題集を提供しています。GoShiken.com NSE7_SDW-6.4 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SDW-6.4 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE7_SDW-6.4-mondaishu.html (**8230%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **47**
管理者は、外部の電話番号に発信するときに発生する VoIP 品質の問題のトラブルシューティングを行っています。エッジ FortiGate の SD-WAN インターフェイスはデフォルト設定で構成されており、2 つのアップストリーム リンクを使用しています。1 つのリンクにはランダムなジッターと遅延の問題があり、ワイヤレスに基づいています。接続 SD_WAN ルールを使用して VoIP 品質を向上させるために、管理者がエッジ FortiGate で同時に適用する必要がある 2 つのアクションはどれですか?

A. 問題のあるリンクをインターフェース優先リストの先頭に置きます。
B. SD-WAN ルールで対応する SD-WAN バランシング戦略を選択します。
C. パフォーマンス SLA ターゲットを使用して、レイテンシーとジッターを即座に検出します。
D. VoIP を使用せずにすべてのトラフィックを負荷分散するように SD-WAN ルールを構成します。
E. インターフェイスのコストと重量に基づいて適切なインターフェイスを選択します
Answer: C,E (メーッセージを残す**)**

最新問題**: 48**
展示を参照してください。

ADVPN を有効にするには何を設定する必要がありますか?
A. ADVPN は、管理対象外の FortiGate デバイスでのみ有効にする必要があります。
B. 保護されたサブネットは、オブジェクトをすべて (0.0 .0. 0/0) にアドレス指定するように設定する必要があります。
C. 各 VPN デバイスには、フェーズ 1 で個別に構成された一意の事前共有キーがあります。
D. ハブ VPN では、デバイスのみが追加のフェーズ 1 セットを必要とします。
Answer: (解答を表示する**)**

最新問題**: 49**
10 Mbps の IP ごとのトラフィック シェーパーをネットワーク全体に適用する方法を定義するステートメントはどれですか?
A. 10 Mbps の帯域幅は IP アドレス間で均等に共有されます。
B. 各 IP には最低 10 Mbps の帯域幅が保証されます。
C. FortiGate は、各 IP アドレスに最大 10 Mbps の帯域幅を割り当てます。
D. 割り当てられた帯域幅をユーザーの総数で割った値を 1 人のユーザーが使用します。
Answer: C (メーッセージを残す**)**
説明/参照:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/885253/per-ip-traffic-shaper

最新問題**: 50**
展示品を参照してください。

Exhibit A | Exhibit B

Edit Policy

Name	Internet Access
Incoming interface	port3
Outgoing interface	SD-WAN
Source	all
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall / Network Options

NAT	
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic
Preserve Source Port	
Protocol Options	PRX default

pdf.com

Exhibit A | Exhibit B

Edit Traffic Shaping Policy

Name: inbound_outbound_shaper

Status: Enabled | Disabled

Comments: Write a comment... 0/255

If Traffic Matches:

Source: all

Destination: all

Schedule:

Service: ALL

Application:

URL Category:

Then:

Action: Apply Shaper | Assign Shaping Class ID

Outgoing interface: SD-WAN

Shared shaper: guarantee-10mbps

jpnpdf.com

図 A はファイアウォール ポリシーを示し、図 B はトラフィック シェーピング ポリシーを示します。
トラフィック シェーピング ポリシーは、すべての送信トラフィックに適用されます。ただし、受信トラフィックはシェーピング ポリシーによって評価されません。
展示内容に基づいて、トラフィック シェーピングを受信トラフィックに適用できるようにするには、どのポリシーでどのような設定変更を行う必要がありますか?
A. リバース シェーパー オプションとして 10mbps 保証オプションを選択する必要があります。
B. 新しいファイアウォール ポリシーを作成し、SD-WAN を受信インターフェイスとして選択する必要があります。
C. リバース シェーパー オプションを有効にし、トラフィック シェーパーを選択する必要があります。
D. IP ごとのシェーパー オプションとして 10mbps 保証オプションを選択する必要があります
Answer: (解答を表示する**)**

最新問題**: 51**
lnkmtd プロセスは何を担当しますか?
A. 処理性能 SLA プローブ
B. ルートタグアドレスのフラッシュ
C. インターフェース品質情報のロギング
D. リンクの帯域幅の飽和を監視します。
Answer: C (メーッセージを残す**)**

最新問題**: 52**
アプリケーション制御を構成するときに SD WAN ルールを使用することが効果的であるのはなぜですか?
A. アプリケーションの種類に基づいてトラフィックの負荷分散ができるため
B. SD-WAIM ルールはファイアウォール ポリシーから独立しているため、アプリケーションの制御を回避できます。
C. ファイアウォール ポリシーで証明書の完全な検査を使用する必要があるため
D. アプリケーション データベースは管理者によって手動で維持されるため
Answer: A (メーッセージを残す**)**
Fortigate によって検出されたアプリケーションに基づいてトラフィックを制御するルールを構成できます。これは、アプリケーション ステアリングまたはアプリケーション対応ルーティングとして知られています。

最新問題**: 53**
展示を参照してください。

出品物から見て、正しい状態説明はどれですか?

A. SD-WAN ルールに一致するトラフィックはポート 2 経由で誘導されます。

B. パケット損失が 10% 未満であるため、ポート 2 は生きています。

C. ポート 1 は SLA ターゲットを満たしていないため、停止しています。

D. SD-WAN メンバーは、さまざまなパフォーマンス SLA によって監視されます。

Answer: A (メーッセージを残す)

最新問題: **54**

管理者は、外部の電話番号に発信するときに発生する VoIP 品質の問題のトラブルシューティングを行っています。エッジ FortiGate の SD-WAN インターフェイスはデフォルト設定で構成されており、2 つのアップストリーム リンクを使用しています。1 つのリンクにはランダムなジッターと遅延の問題があり、ワイヤレスに基づいています。接続 SD_WAN ルールを使用して VoIP 品質を向上させるために、管理者がエッジ FortiGate で同時に適用する必要がある 2 つのアクションはどれですか?

A. SD-WAN ルールで対応する SD-WAN バランシング戦略を選択します。

B. パフォーマンス SLA ターゲットを使用して、レイテンシーとジッターを即座に検出します。

C. インターフェイスのコストと重量に基づいて、適切なインターフェイスを選択します。

D. VoIP を使用せずにすべてのトラフィックを負荷分散するように SD-WAN ルールを構成します。

E. 問題のあるリンクをインターフェース優先リストの先頭に置きます。

Answer: (解答を表示する)

最新問題: **55**

展示を参照してください。

VPN トンネルのステータスに関する 2 つの記述のうち、正しいものはどれですか? <2つ選択してください)

A. FortiGate は、すべてのクライアントによって共有される単一の IPsec 仮想インターフェイスを作成しました。

B. ダイヤルアップ クライアントごとに個別の仮想インターフェイスがあります。

C. 100.64.3.1 は、インデックス インターフェイス 1 を介して送信されるリモート IP アドレスの 1 つです。

D. VPN 静的ルートは FortiGate ルーティング テーブルに追加されません。

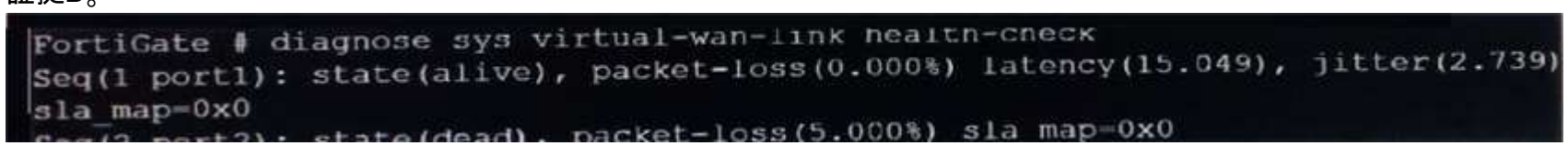
Answer: A,C (メーッセージを残す)

最新問題: **56**

展示品を参照してください。

証拠品A。

証拠B。



資料 A は SD-WAN パフォーマンス SLA を示し、資料 B は参加している SD-WAN メンバーの健全性を示しています。

展示物に基づいて、どの記述が正しいでしょうか?

A. チェック間隔は、メンバー インターフェイスによって送信されたパケットが失われたとみなされるまでの待機時間です。

B. ポート 2 はステータスがアライブからデッドに変わるまで 500 ミリ秒待つ必要があります。

C. デッド メンバー インターフェイスは、管理者が手動でインターフェイスを戻すまで使用できません。

D. ポート 2 の SLA 状態が、SLA サーバーからの未応答リクエストが連続 3 回を超えました。
Answer: D (メーッセージを残す)

最新問題: **57**
デフォルトの SD-WAN 最小構成において、トラフィックがデフォルトの暗黙的な SD-WAN ルールに一致する場合に正しい 2 つの記述はどれですか? (2つお選びください)
A. 絶対的な SD-WAN ルールが定義され、トラフィックと一致しました。
B. 一致したトラフィックが RPF に失敗し、ルールによってキャッチされました。
C. トラフィックはどの FortiGate ポリシー ルートにも一致しませんでした。
D. FIB ルックアップで解決されたインターフェイスは SD-WAN インターフェイスでした。
Answer: C,D (メーッセージを残す)

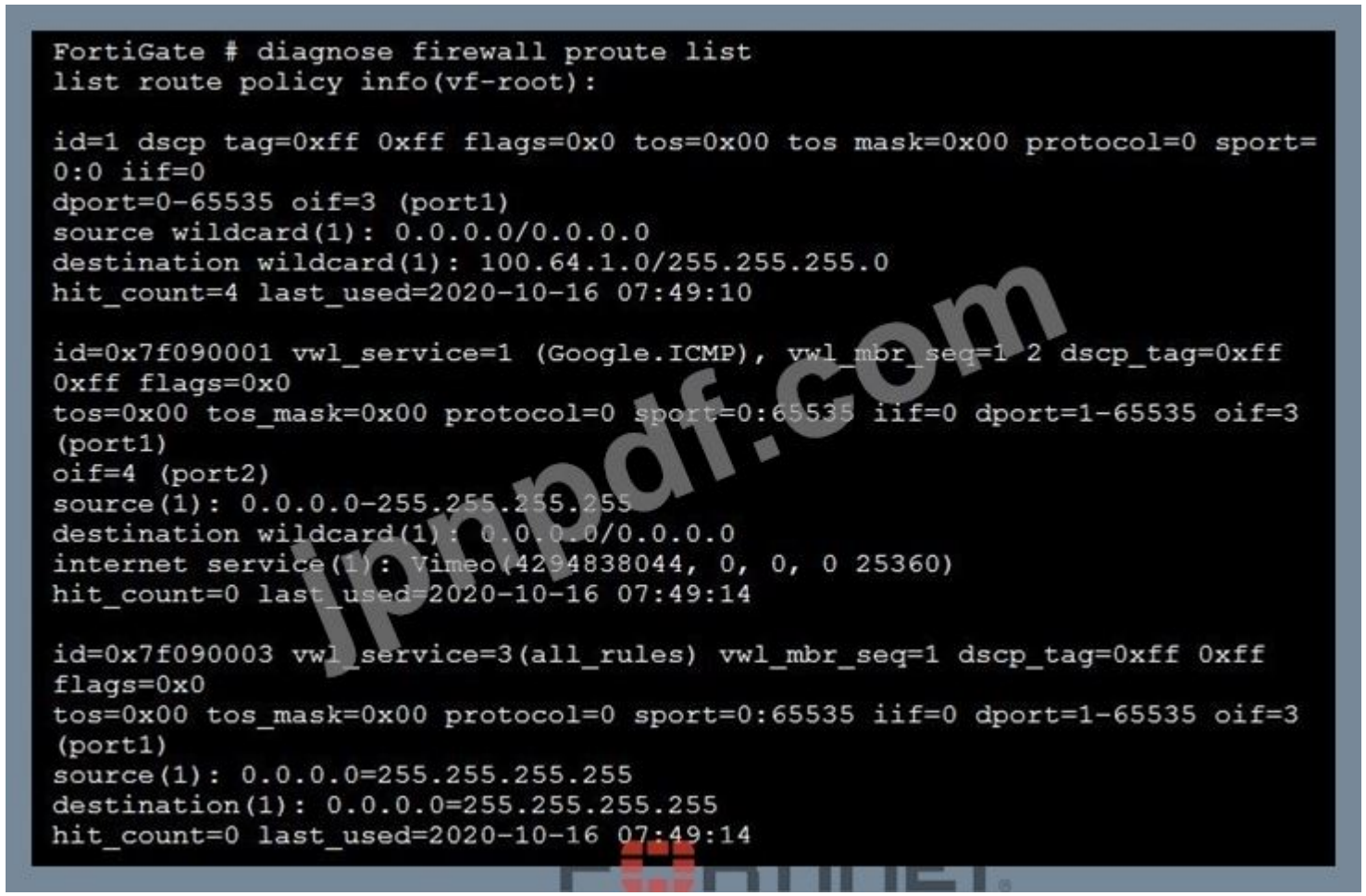
最新問題: **58**
SD-WAN と ADVPN について正しいのはどれですか?
A. ADVPN ショートカットのルートは手動で構成する必要があります。
B. SD-WAN は、SD-WAN メンバーとして構成された IPsec オーバーレイ上に確立された ADVPN ショートカットにトラフィックを誘導できます。
C. SD-WAN は、ADVPN ショートカットの正常性とパフォーマンスを監視しません。
D. OSPF を使用する必要があります。
Answer: B (メーッセージを残す)

最新問題: **59**
展示を参照してください。

2 つのハブアンドスポーク グループ間、およびハブ 1 とハブ 2 の間のサイト間で複数の IPsec VPN が形成されています。管理者はデュアル リージョン トポロジで ADVPN を構成しました。トロントとロンドンは設立されましたか？(2つお選びください)
A. すべての VPN インターフェイスで auto-discovery-forwarder IS が有効になっています
B. トンネルサーチ IS をフェーズ 2 クイック モード セレクターに設定
C. auto-discovery-receiver がスポークの出力 VPN インターフェイスで有効になっています
D. ハブの入力 VPN インターフェイスで自動検出送信者が有効になっています
E. add-route が有効になり、ハブ デバイスにスタティック ルートをインストールできます。

Answer: C,D (メーッセージを残す)

最新問題: **60**
展示を参照してください。



出力に基づいて、正しい結論は 2 つありますか? (2つお選びください。)
A. エントリ 1 (id=1) は通常のポリシー ルートです。
B. SD-WAN ルールは、通常のポリシー ルートよりも優先されます。
C. all_rules ルールは、暗黙的な SD-WAN ルールを表します。
D. 複数の SD-WAN ルールが設定されています。
Answer: (解答を表示する)

最新問題: **61**
展示を参照してください。

```
config vpn ipsec phase1-interface
   edit "FIRST_VPN"
      set type dynamic
      set interface "port1"
      set peertype any
      set proposal aes128-sha256 aes256-sha38
      set dhgrp 14 15 19
      set xauthtype auto
      set authusrgrp "first-group"
      set psksecret fortinet1
   next
   edit "SECOND_VPN"
      set type dynamic
      set interface "port1"
      set peertype any
      set proposal aes128-sha256 aes256-sha38
      set dhgrp 14 15 19
      set xauthtype auto
     set authusrgrp "second-group"
     set psksecret fortinet2
   next
edit
```

jpn.pdf.com

FortiGate には、FIRST_VPN のみに一致する port1 に着信する複数のダイヤルアップ VPN インターフェイスがあります。
受信接続がすべての可能な IPsec ダイヤルアップ インターフェイスと一致できるようにするには、両方の IPsec VPN インターフェイスに対して行う必要がある 2 つの設定変更はどれですか? (2つお選びください。)
A. 各 VPN インターフェイスで固有の Diffie Hellman グループを使用します。
B. IKE モードをアグレッシブ モードに設定します。
C. 各ダイヤルアップ VPN インターフェイスに一意のピア ID を指定します。
D. インターフェース間で異なるプロポーザルが使用されます。
Answer: A,D (メーッセージを残す)

有効な **NSE7_SDW-6.4** 問題集は GoShiken.com が提供された合格しやすい NSE7_SDW-6.4 試験問題集！ GoShiken.com が最新の **NSE7_SDW-6.4** 試験問題集を提供しています。GoShiken.com NSE7_SDW-6.4 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SDW-6.4 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE7_SDW-6.4-mondaishu.html (**8230%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

Valid NSE7_SDW-6.4 Dumps shared by GoShiken.com for Helping Passing NSE7_SDW-6.4 Exam! GoShiken.com now offer the **newest NSE7_SDW-6.4 exam dumps**, the GoShiken.com NSE7_SDW-6.4 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com NSE7_SDW-6.4 dumps with Test Engine here:

https://www.goshiken.com/Fortinet/NSE7_SDW-6.4-mondaishu.html (**82** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)