PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **FCSS_SDW_AR-7.4-JPN**

Title : FCSS - SD-WAN 7.4 Architect (FCSS_SDW_AR-7.4日本語版)

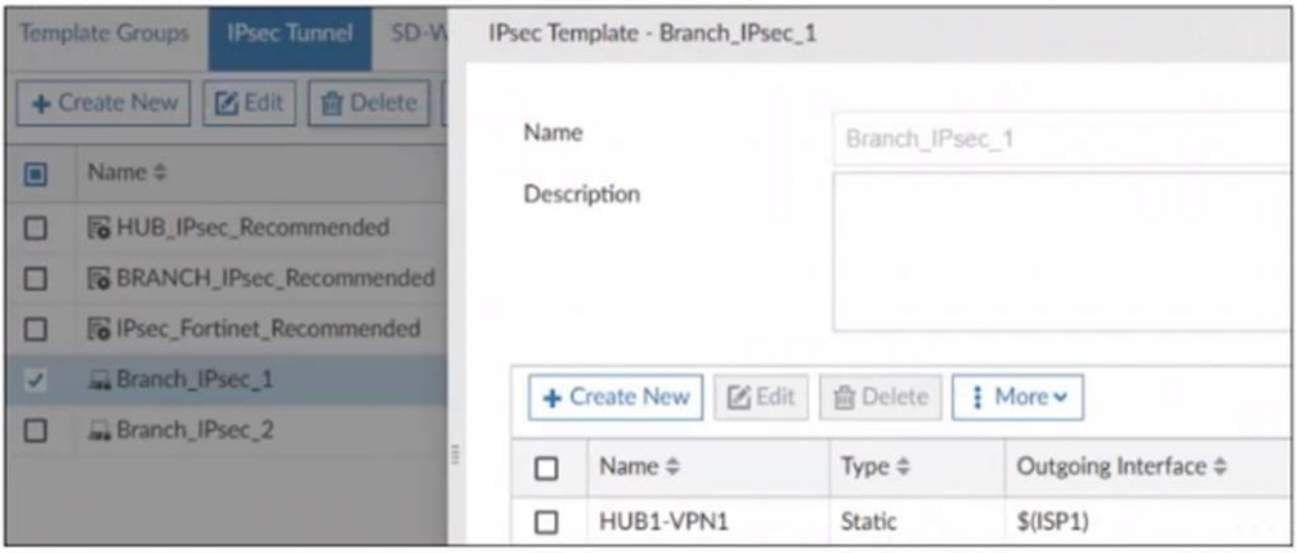
Vendor : Fortinet

Version : DEMO

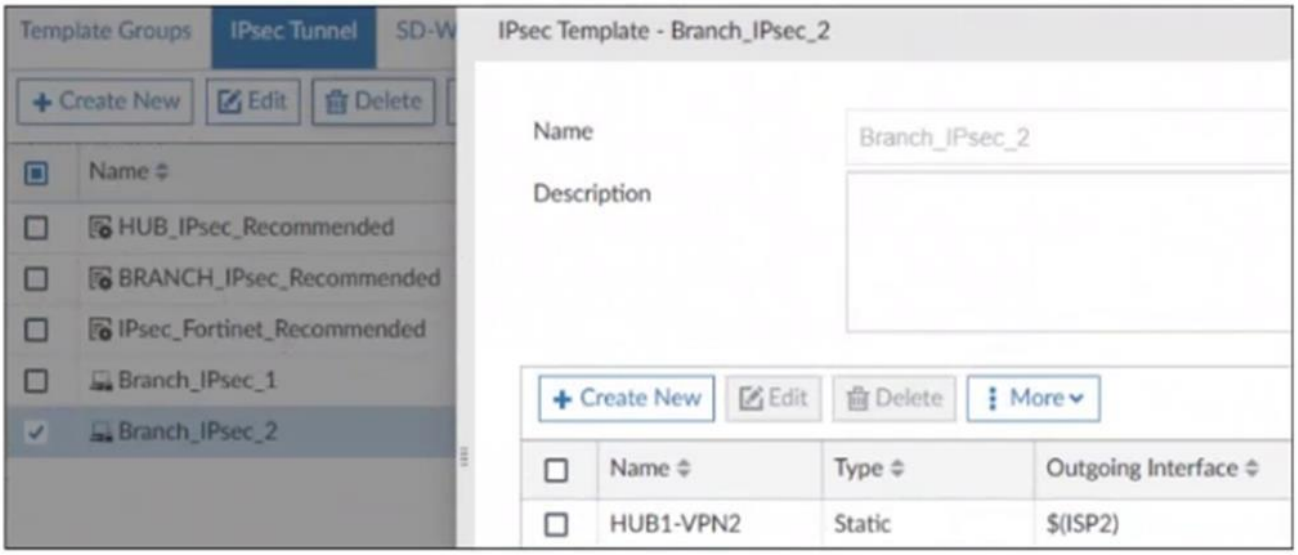
QUESTION NO: 1
既にADVPNが設定されているSD-WANトポロジにADVPN 2.0を設定するという課題があります。このシナリオでADVPN 2.0を実装するにはどうすればよいでしょうか？
A. ハブ上の IPsec トンネル構成を更新します。
B. ブランチの SD-WAN 構成を更新します。
C. ブランチ上の IPsec トンネル構成を更新します。
D. 既存の ADVPN 構成を削除し、ADVPN 2.0 を構成します。
Answer: A
Explanation:
To implement ADVPN 2.0 on an existing ADVPN topology, you only need to update the IPsec tunnel configuration on the hub to support the enhanced capabilities. Branch configurations remain unchanged.

QUESTION NO: 2
添付資料を参照してください。添付資料には、Branch IPsec 1とBranch_IPsec_2を定義する2つのIPsecテンプレートが示されています。各テンプレートはVPNトンネルを定義しています。管理者が2つ目のテンプレートをFortiGateデバイスに割り当てようとしたときにFortiManagerに表示されたエラーメッセージも示されています。問題の原因を最もよく表しているのはどれですか？

IPsec template for Branch_IPsec_1



IPsec template for Branch_IPsec_2



Error message in FortiManager

A. 各 FortiGate デバイスには、トンネル タイプが静的であるテンプレートを 1 つだけ割り当てることができます。
B. 各 FortiGate デバイスに割り当てることができる IPsec テンプレートは 1 つだけです。
C. rootVDOM に設定されているトンネルの branch1_fgt 設定を確認する必要があります。
D. 両方のテンプレートで同じ送信インターフェイスを使用する必要があります。

Answer: B

Explanation:

FortiManager allows only one IPsec template to be assigned per FortiGate device. The error indicates a conflicting template assignment, meaning assigning both Branch_IPsec_1 and

Branch_IPsec_2 to the same device (branch1_fgt) is not permitted.

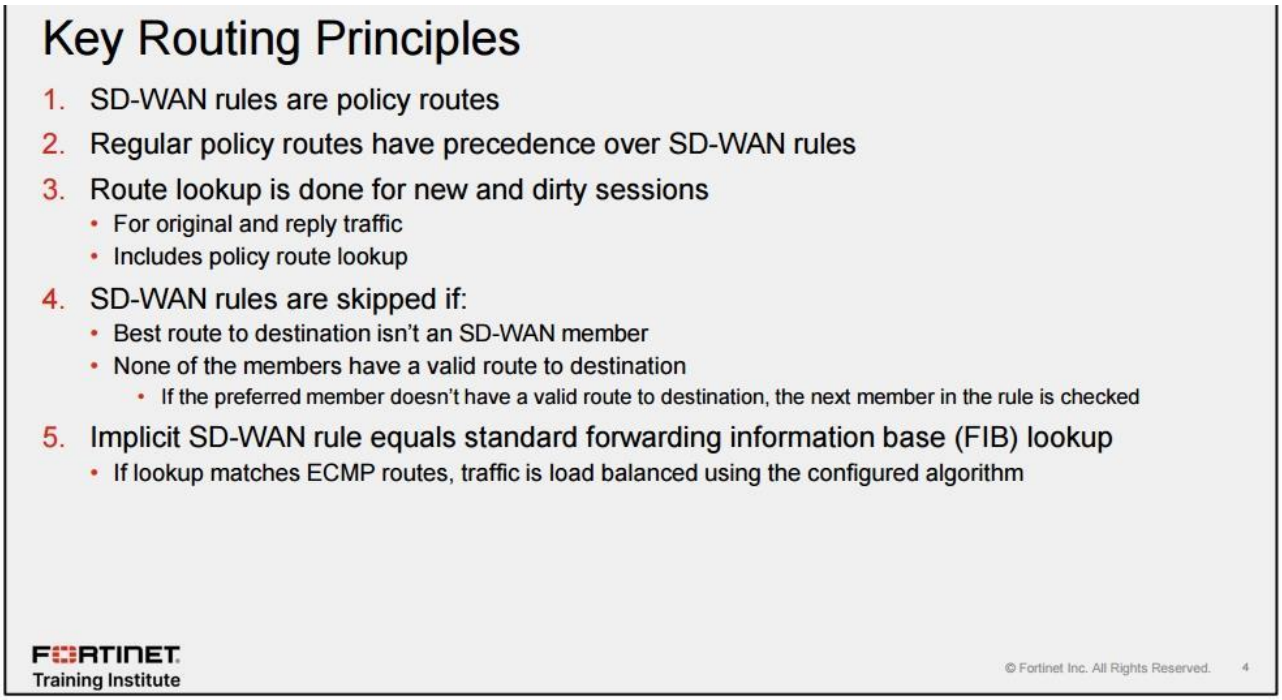
QUESTION NO: 3
図を参照してください。管理者がFortiGate上のSD-WANのトラブルシューティングを行っています。branch1_fgtの背後にあるデバイスが10.0.0.0/8ネットワークへのトラフィックを生成します。
管理者は、トラフィックが SD-WAN ルール ID 1 に一致し、HUB1-VPN1 経由でルーティングされることを期待しています。
ただし、トラフィックは HUB1-VPN3 経由でルーティングされます。
展示に示されている出力に基づいて、観察された動作を説明できる 2 つの理由 (個別または組み合わせ) はどれですか。(2 つ選択してください。)

Diagnose output

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority: 2
      Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535), Mode(sla), sla-compare-order
      Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
          2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
          3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
     Src address(1):
          10.0.1.0-10.0.1.255

fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd may_child, gateway: 100.64.1.1, peer:
192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd may_child, gateway: 100.64.1.9, peer:
192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd may_child, gateway: 172.16.1.5, peer:
192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0

fgt_A # get router info routing-table all | grep HUB1
S         10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B         10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41,
[1/0]
                      [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41,
[1/0]
B         10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42. [1/0]
                      [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42. [1/0]
                      [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42. [1/0]
```

A. HUB1-VPN3のメンバー構成優先度はHUB1-VPN1よりも高い
B. トラフィックは、HUB1-VPN3を送信デバイスとして設定した通常のポリシールートと一致します。
C. HUB1-VPN1には宛先への有効なルートがありません
D. HUB1-VPN3 のルート優先度値は HUB1-VPN1 よりも低く (優先度が高く) なっています。

Answer: BC
Explanation:



QUESTION NO: 4
FortiGateは本番環境で稼働しています。WANリンクの使用を最適化し、冗長性を向上させるために、SD-WANを有効化して設定します。
この構成更新プロセスの一環として何を行う必要がありますか?
A. ルーティング構成で SD-WAN
メンバーとして使用されるインターフェイスへの参照を置き換えます。
B. SD-WAN ライセンスを購入してインストールし、FortiGate デバイスを再起動します。
C. ファイアウォール ポリシーで SD-WAN
メンバーとして使用されるインターフェイスへの参照を置き換えます。
D. SD-WAN メンバーとして使用するインターフェースを無効にします。
Answer: A
Explanation:
When you enable SD-WAN and add interfaces as SD-WAN members, those interfaces are no longer referenced directly in routing. You must replace routing configuration references (e.g., static routes, policy routes) with the SD-WAN zone. Firewall policies, however, can still point to the SD-WAN zone without requiring replacement of individual member interfaces.

QUESTION NO: 5
添付資料を参照してください。FortiManagerを使用してブランチデバイスの管理とSD-WANテンプレートの設定を行い、IT部門ユーザー向けにダイレクトインターネットアクセス（DIA）を設定しました。
ここで、すべてのローカル LAN ユーザーに対してセキュア インターネット アクセス (SIA) を構成し、2 番目の図に示すようにファイアウォール ポリシーを設定する必要があります。その後、インストールウィザードを使用してブランチデバイスに設定とポリシーパッケージをインストールすると、FortiManagerは3番目の図に示すようにエラーを報告します。FortiManagerがブランチに設定をインストールできなかった理由を説明する記述はどれですか？

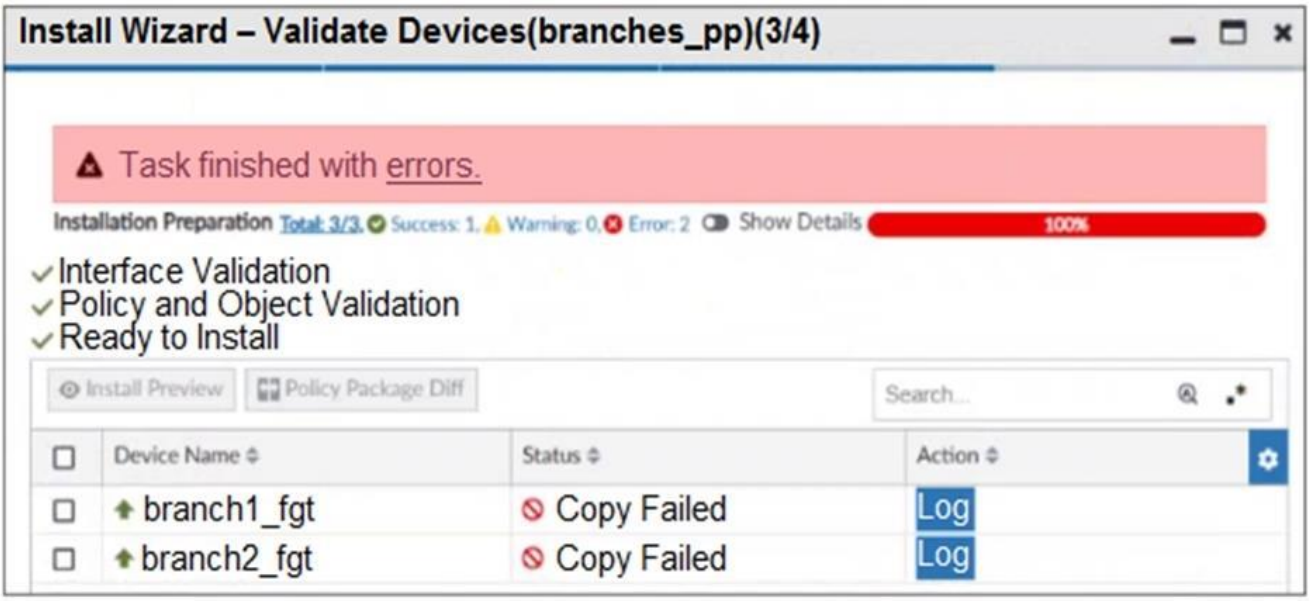
SD-WAN template on FortiManager

Name	Assigned to Device/Group	Interface
branches	2 Devices in Total View Details > branch1_fgt [root] branch2_fgt [root]	port1 port2

Firewall policies

Underlay (2/3 Total:2)									
2	SIA	LAN	port1	LAN-net	all	always	FTP HTTP HTTPS	Accept	no-inspection default
3	DIA	LAN	underlay	LAN-IT	all	always	ALL	Accept	default certificate-i... default

FortiManager error message



A. SIA トラフィックを VPN トンネルに送信する必要があります。
B. SD-WAN ゾーンを参照するファイアウォール
ポリシーをインストールすることはできません。
C. SD-WAN メンバーを参照するファイアウォール
ポリシーをインストールすることはできません。
D. 同じデバイスに SIA ルールと DIA ルールをインストールすることはできません。
Answer: C
Explanation:
In FortiManager, firewall policies must reference SD-WAN zones, not individual SD-WAN members (interfaces like port1 or port2). The SIA rule incorrectly references port1, which is a member - not a zone - causing the installation failure during validation.

QUESTION NO: 6
SD-WAN オーバーレイテンプレートは、SD-WAN 導入の準備に役立ちます。SD-WAN オーバーレイテンプレートによって実行されるタスクを完了するには、管理者が実行後のタスクをいくつか実行する必要があります。
実行後に必ず実行する必要がある 2 つの必須タスクは何ですか? (2 つ選択してください)
A. SD-WAN オーバーレイ テンプレートによって作成されたオーバーレイ トンネルを介したルーティングを構成します。
B. ポリシー パッケージを作成し、ブランチ デバイスに割り当てます。
C. 各ハブ デバイスにハブ ID メタデータ変数を割り当てます。
D. SD-WANルールを構成する
E. 各デバイス (ブランチとハブ) に sdwan_id メタデータ変数を割り当てます。
Answer: BD
Explanation:
On page 76 in the Study Guide:
"You must define a unique branch ID value for each branch device"
"Mandatory . . .
- Configure the SD-WAN rules by editing the SD-WAN template
- Create policy packages for branch and hub devices"

QUESTION NO: 7
添付資料を参照してください。管理対象FortiGateデバイスのインターフェースの詳細、静的ルート設定、ファイアウォールポリシーが表示されます。
インターフェイス port1 と port2 を含む、Underlay という名前の新しい SD-WAN ゾーンを設定します。
あなたの最初の行動は何でしょうか?

Interface details

Name	Type	Members	IP/Netmask
Physical Interface 13			
port1	Physical Interface		192.2.0.1/255.255.255.248
port2	Physical Interface		192.2.0.9/255.255.255.248
port3	Physical Interface		0.0.0.0/0.0.0.0
port4	Physical Interface		172.16.0.1/255.255.255.248
port5	Physical Interface		10.0.1.254/255.255.255.0
port6	Physical Interface		0.0.0.0/0.0.0.0
port7	Physical Interface		0.0.0.0/0.0.0.0
port8	Physical Interface		0.0.0.0/0.0.0.0
port9	Physical Interface		0.0.0.0/0.0.0.0
port10	Physical Interface		192.168.0.31/255.255.255.0
T_shop_1(port9)	Physical interface		0.0.0.0/0.0.0.0
SD-WAN Zone 3			
HUB1	SD-WAN Zone	HUB1-VPN1 HUB1-VPN2 HUB1-VPN3	0.0.0.0/0.0.0.0
Test	SD-WAN Zone	port2	0.0.0.0/0.0.0.0
virtual-wan-link	SD-WAN Zone		0.0.0.0/0.0.0.0

Static route details

Destination	Gateway IP	Interface	Status
192.168.1.0/24	192.2.0.254	port1	Enabled
168.1.1.0/24	192.2.0.4	port1	Enabled

Firewall policies on managed FortiGate

	Policy	From	To	Source	Destination	Service
☐	Corp(5)	port1	port5	Corp-net	LAN-net	HTTP HTTPS
☐	DIA(1)	port5	port1	LAN-net	all	ALL

A. ポート1をSD-WANメンバーとして定義します。
B. 静的ルートを削除します。
C. SD-WAN ゾーン テストを削除します。
D. ファイアウォール ポリシーを削除します。
Answer: C
Explanation:
In the exhibits, port2 is already assigned to the SD-WAN zone named Test. An interface can only belong to a single SD-WAN zone, so before you can add both port1 and port2 into the new SD- WAN zone Underlay, you must first delete the SD-WAN Zone Test to free port2.

QUESTION NO: 8
SD-WANは他の多くのFortiGate機能と連携します。これらの機能の一部は、SD-WANによるトラフィック制御に必須です。
FortiGate が SD-WAN ルールに従ってトラフィックを誘導する前に設定する必要がある 3 つの構成要素はどれですか (3 つ選択してください)。
A. ファイアウォールポリシー
B. インターフェース
C. セキュリティプロファイル
D. トラフィックシェーピング
E. ルーティング
Answer: ABE
Explanation:
Interfaces must be defined and added as SD-WAN members to participate in traffic steering. Routing is required so FortiGate knows how to reach destinations through SD-WAN paths. Firewall policies are needed to permit traffic and allow SD-WAN rules to take effect.