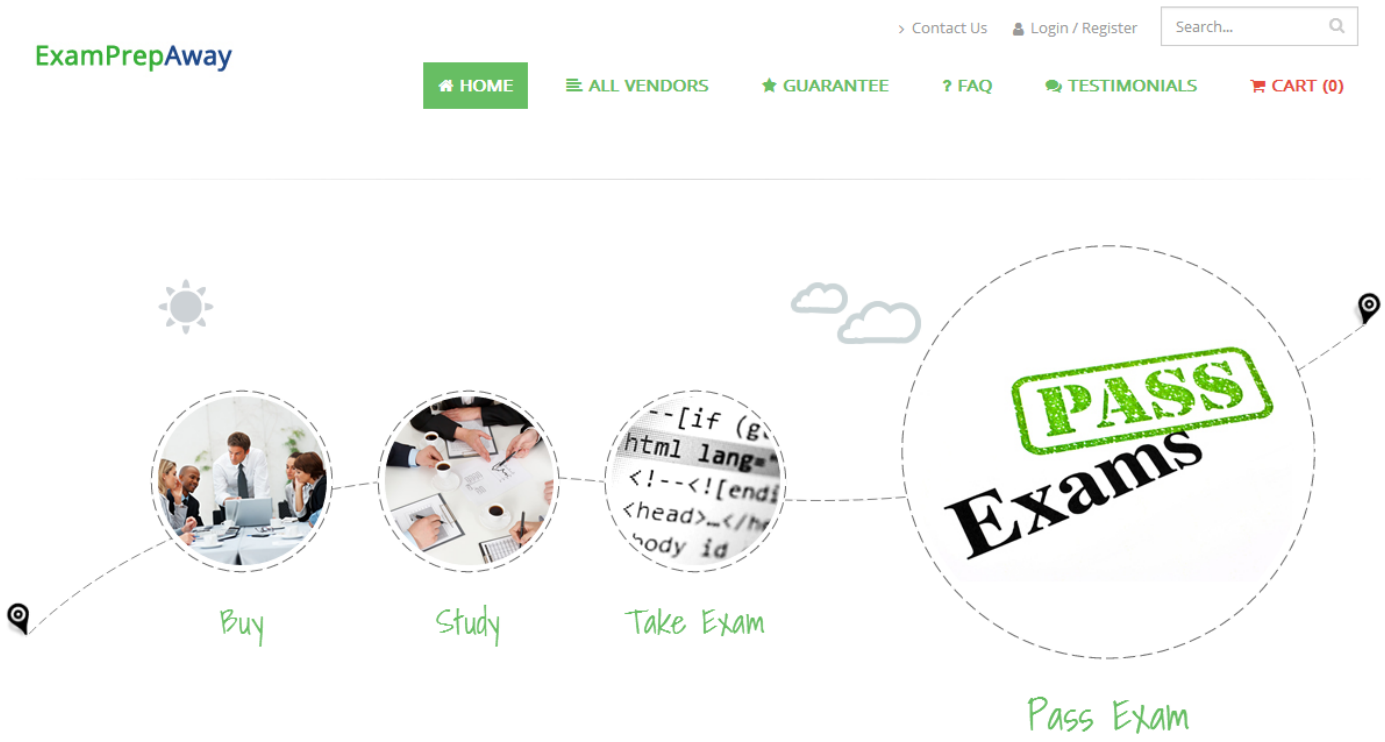
ExamPrepAway



Try **Online Engine** before you buy

We're not the only ones **happy** about ExamPrepAway Practice Material ...

56295+ customers in 100+ countries use ExamPrepAway Test Engine. Meet our customers.

GetCustom JET ORANGE iCompany Paradoxx iMessenger VOREED

http://www.examprepaway.com/

Latest Exam Guide & Learning Materials

Exam : **NSE7_SDW-7.2-JPN**

Title : Fortinet NSE 7 - SD-WAN 7.2 (NSE7_SDW-7.2日本語版)

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
FortiGate がゼロタッチ プロビジョニング プロセスを完了できない 2 つの理由は何ですか? (2つ選択してください。)
A. FortiGate クラウド キーが FortiGate クラウド ポータルに追加されていません。
B. FortiDeploy は FortiGate に接続し、FortiManager に接続するための初期構成を提供しました
C. ゼロタッチプロビジョニングプロセスが FortiGate の背後で内部的に完了しました。
D. FortiGate は FortiGate クラウドのプラットフォーム テンプレートから構成を取得しました。
E. FortiGate で工場出荷時設定へのリセットが実行されました。
Answer: A C

QUESTION NO: 2
IPsec 推奨テンプレートを使用してハブアンドスポーク トポロジで IPsec トンネルを構成する 2 つの利点は何ですか? (2 つ選択してください。)
A. VPN モニター ツールは、IPsec 推奨テンプレートで定義されたトンネルの追加統計情報を提供します。
B. FortiManager は、スポークが FortiManager ADOM に追加されると、すべてのスポークに IPsec トンネルを自動的にインストールします。
C. IPsec 推奨テンプレートは、管理者が Fortinet 推奨設定を使用するようにガイドします。
D. IPsec 推奨テンプレートにより、フェーズ 1 とフェーズ 2 の間で一貫した設定が保証されます。
Answer: B C
Explanation:
According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:
* FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM. This reduces the manual effort and ensures that all spokes have the same configuration.
* IPsec recommended template guides the administrator to use Fortinet recommended settings, such as encryption algorithms, key lifetimes, and dead peer detection. This ensures optimal performance and security of the IPsec tunnels.

QUESTION NO: 3
どの 2 つのインターフェースがオーバーレイ リンクと見なされますか? (2 つ選択してください。)
A. ラグ
B. IPsec
C. 物理
D. GRE
Answer: B D

QUESTION NO: 4

展示を参照してください。

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(3 T_INET_0_0), alive, selected
    2: Seq_num(4 T_INET_1_0), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S       10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

管理者は、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は、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、T_INET_0_0
経由でルーティングされると予想しています。しかし、トラフィックは T_INET_1_0
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、観察された動作を引き起こす可能性のある 2 つの理由はどれですか? (2 つ選択してください。)

A. トラフィックは、T_INET_1_0 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。

B. T_INET_1_0 のルート優先度値は T_INET_0_0 よりも低く (優先度が高く) なっています。

C. T_INET_0_0 には宛先への有効なルートがありません。

D. T_INET_1_0 のメンバー構成の優先順位は T_INET_0_0 よりも高くなっています。

Answer: A C

Explanation:
SD-WAN strategy is Lowest Cost (SLA) as indicated by the "Mode(sla)" flag. Cost SLA uses SLA target, cost, and priority (i.e., interface preference - or order of config unless manually overridden by admin config) as the criteria -- in that order. Both members meet the target, both have 0 cost, and therefore member 3 (T_INET_0) wins the "priority" tiebreaker. So if there is a valid route to the destination through member 3, it will win. The fact that it does not has nothing to do with the configured static route/member priority, which according to SG page 197 "is used as a tiebreaker for ECMP routes when matching implicit SD-WAN rule."

QUESTION NO: 5
展示品を参照してください。
証拠書類A

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

証拠書類B

```
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
          members(2): 3(port1) 4(port2)
```

図 A は、SD-WAN パフォーマンス SLA 構成、SD-WAN ルール構成、Facebook および YouTube のアプリケーション ID を示しています。図 B は、ファイアウォール ポリシー構成とアンダーレイ ゾーンのステータスを示しています。
展示物に基づいて、ポート 1 とポート 2 の健全性とパフォーマンスについて正しい 2 つの記述はどれですか。
（2つ選択してください。）

A. パフォーマンスは、メンバーを通過する Facebook および YouTube トラフィックについて測定された指標の平均です。

B. FortiGate は、Facebook および YouTube トラフィックのジッターとパケット損失を測定できません。

C. Facebook および YouTube のトラフィックがメンバーを通過していない場合、FortiGate はメンバーがデッド状態であると識別します。

D. 非 TCP Facebook および YouTube トラフィックはパフォーマンス測定には使用されません。

Answer: A D

Explanation:
Study Guide 7.2, pages 103 - 104. Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

QUESTION NO: 6

スポークの IPsec フェーズ 1 構成を示す図を参照してください。

```
config vpn ipsec phase1-interface
    edit "T_INET_0_0"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "[created by FMG VPN Manager]"
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret ENC
6D5rVsaK1MeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc51tCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH01SPFKz5IYCVA==
    next
end
```

ADVPN を SD-WAN で動作させるには、IPsec フェーズ 1 構成で何を構成する必要がありますか?

A. ike-version を 1 に設定する必要があります。

B. net-device を有効にする必要があります。

C. 自動検出送信者を有効にする必要があります。

D. アイドルタイムアウトを無効にする必要があります。

Answer: B

QUESTION NO: 7

リモート インターネット アクセス (RIA) の一般的な使用例を 2 つ挙げてください。(2 つ選択してください。)

A. スポーク上で直接インターネットアクセスを提供する

B. ハブ経由でインターネットアクセスを提供する

C. ハブ上でセキュリティ検査を集中管理する

D. スポークを徹底的に検査する

Answer: B C

Explanation:

B: Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.

C: Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

QUESTION NO: 8

展示品を参照してください。

Exhibit A

	#	Name	From	To	Source	Destination
☑	1	DIA	D-LAN LAN	underlay	LAN-net	all
☐	Implicit (2/2 Total:1)					
☐	2	Implicit Deny	any	any	all all	all all

Exhibit B

View Install Log

```
Copy device global objects

validation error on firewall policy 1, by dynamic interface check

Vdom copy failed:
error 42 - entry not exist. detail: Dynamic interface "LAN" mapping undefined for device branch2_fgt

Copy objects for vdom root
```

図 A はポリシー パッケージの定義を示しています。図 B は、管理者が FortiGate デバイスにポリシー パッケージをインストールしようとしたときに受け取ったインストール ログを示しています。
展示物に示された出力に基づいて、管理者は問題を解決するために何ができるでしょうか?
A. インストール ターゲット リスト内のすべてのデバイスの LAN インターフェイスの動的マッピングを作成します。
B. ファイアウォール ポリシーを定義するには、動的インターフェイスの代わりにメタデータ変数を使用します。
C. 動的マッピングは自動的に実行されるはずです。branch2_fgt の LAN インターフェイス構成を確認してください。
D. ポリシーは 1 つの LAN ソース インターフェイスのみを参照できます。動的 LAN インターフェイスである D-LAN のみを保持します。
Answer: A

QUESTION NO: 9
展示を参照してください。

```
config system interface
    edit "port2"
        set vdom "root"
        set ip 192.2.0.9 255.255.255.248
        set allowaccess ping
        set type physical
        set role wan
        set snmp-index 2
        set preserve-session-route enable
    next
end
```

図に基づいて、FortiGate はポート 2 を通過するトラフィックに対してどの 2 つのアクションを実行しますか? (2 つ選択してください。)

A. FortiGate は、ルート変更後、有効なゲートウェイを使用する既存のセッションのルーティング情報を変更しません。

B. FortiGate は、ルート変更後に、新しいセッションに対してのみルーティング ルックアップを実行します。

C. ルート変更後、FortiGate は常にすべてのトラフィックをブロックします。

D. ルート変更後、FortiGate はセッション テーブルからすべてのルーティング情報をフラッシュします。

Answer: A B

QUESTION NO: 10

IPsec スイートのどの 2 つのプロトコルが認証と暗号化に最もよく使用されますか? (2 つ選択してください。)

A. カプセル化セキュリティペイロード (ESP)

B. セキュア シェル (SSH)

C. インターネット鍵交換 (IKE)

D. セキュリティ アソシエーション (SA)

Answer: A C